

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

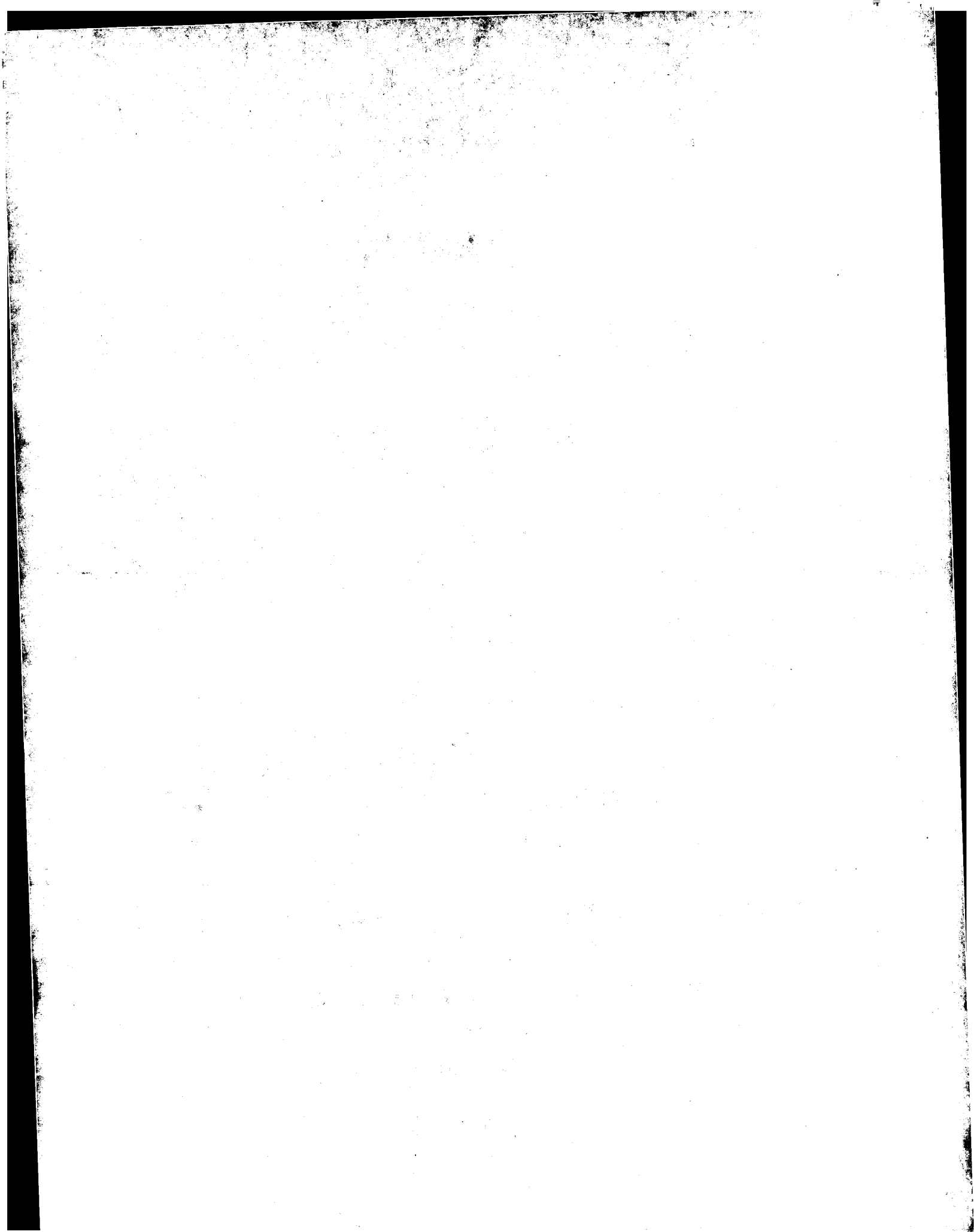
Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.**



## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-349725

(43)Date of publication of application : 15.12.2000

(51)Int.Cl.

H04H 1/00

H04B 1/16

H04L 9/08

H04L 9/36

H04N 5/44

H04N 7/16

(21)Application number : 11-158212

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 04.06.1999

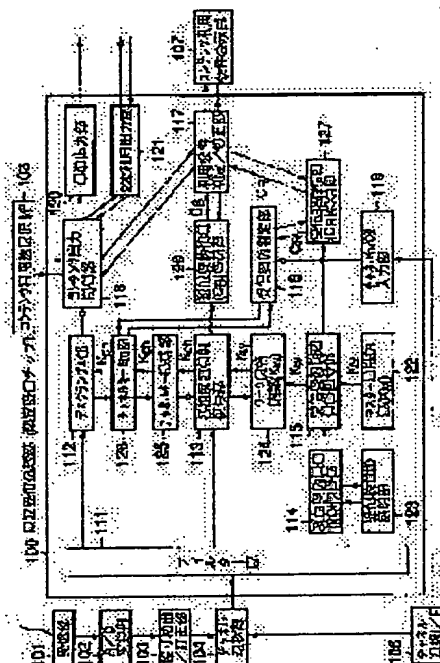
(72)Inventor : AKIYAMA KOICHIRO

## (54) BROADCAST RECEPTION DEVICE AND CONTENT USE CONTROL METHOD

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To control use of every content by synthesizing first use condition information common to a plurality of pieces of content information and second use condition information which is broadcast in accordance with the plurality of pieces of content information and is common to a plurality of contractors, deciding a use condition on designated content information and controlling the use of corresponding content information.

**SOLUTION:** Priority is given to individual conditions and an order is given to unified content use conditions in accordance with the priority and the contract use condition of the highest priority is set to be a corrected use condition. Since first priority is given to the limit of the number of items, a use possible contract information list is referred to from the limit of the number of times. When use possible contract information satisfying the condition does not exist, the use possible contract information list having the largest number of designation of limit information on the number of times is extracted and the list is similarly generated. The contract condition whose period is the longest is extracted and the corrected content use condition is generated.



## LEGAL STATUS

[Date of request for examination]

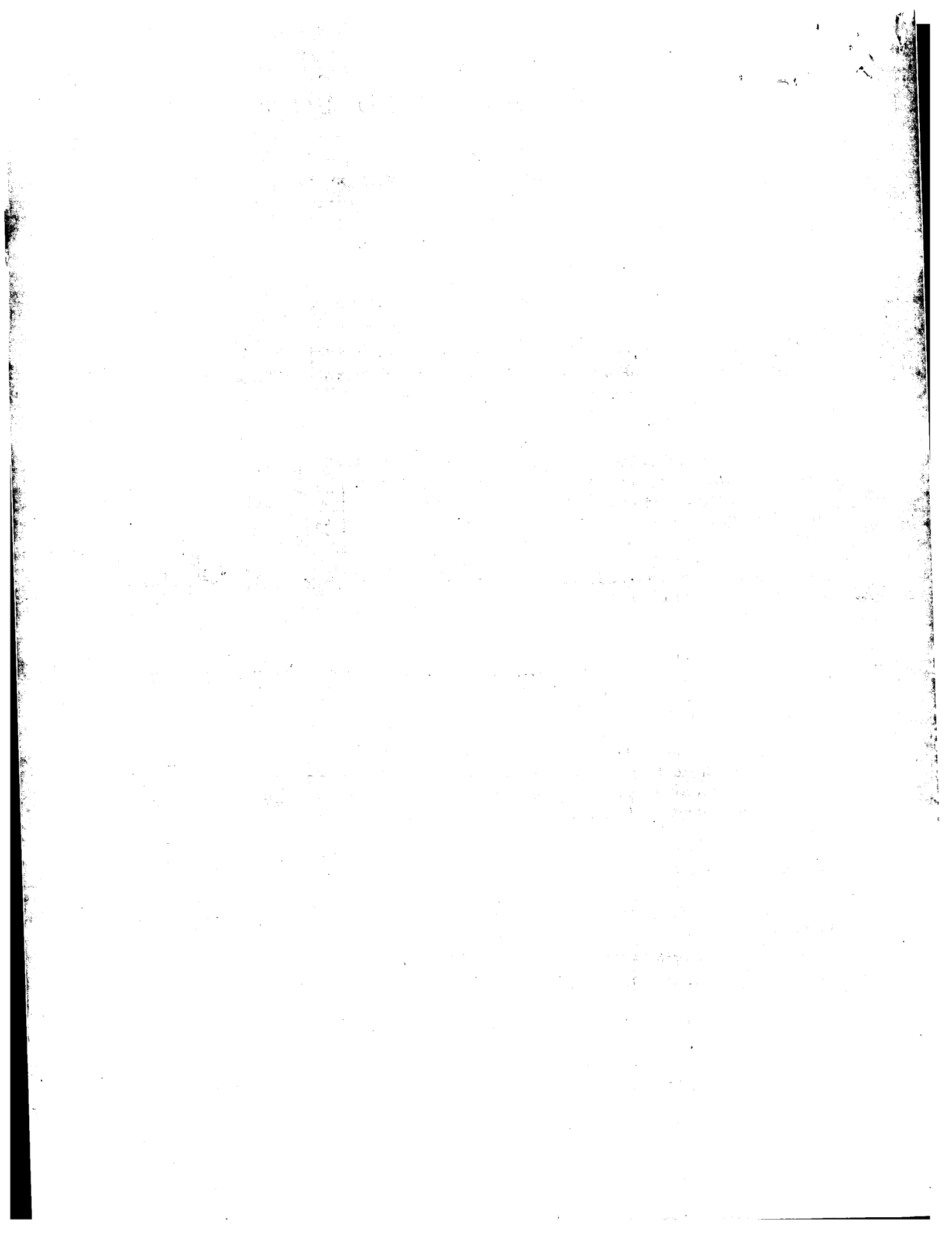
12.09.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]



[Date of registration]

[Number of appeal against examiner's decision  
of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office



(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号  
特開2000-349725  
(P2000-349725A)

(43)公開日 平成12年12月15日(2000.12.15)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テマコード(参考)
H 0 4 H 1/00		H 0 4 H 1/00	F 5 C 0 2 5
H 0 4 B 1/16		H 0 4 B 1/16	G 5 C 0 6 4
H 0 4 L 9/08		H 0 4 N 5/44	D 5 J 1 0 4
		7/16	Z 5 K 0 6 1
H 0 4 N 5/44		H 0 4 L 9/00	6 0 1 A

審査請求 未請求 請求項の数13 O L (全 38 頁) 最終頁に続く

(21)出願番号 特願平11-158212

(22)出願日 平成11年6月4日(1999.6.4)

(71)出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72)発明者 秋山 浩一郎

神奈川県川崎市幸区小向東芝町1番地 株  
式会社東芝研究開発センター内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

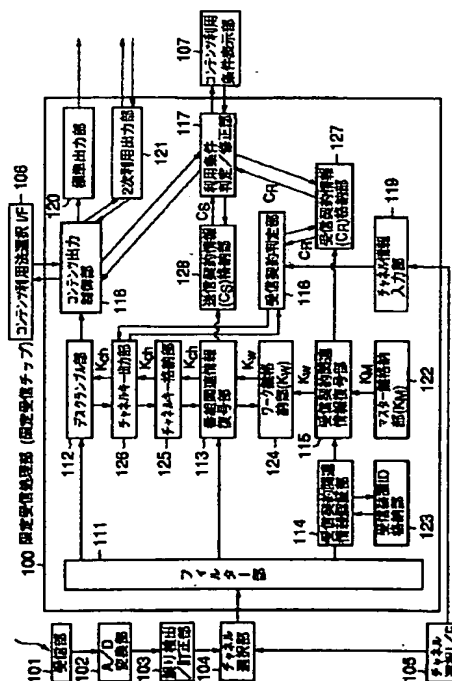
最終頁に続く

(54) 【発明の名称】 放送受信装置及びコンテンツ利用制御方法

(57) 【要約】

【課題】 放送コンテンツに応じて2次利用を制御可能な放送受信装置を提供すること。

【解決手段】 放送配信されるコンテンツ情報の利用を  
利用条件に応じて制御する放送受信装置であって、個々  
の契約者に対応して放送される、同じチャネルに含まれ  
る複数のコンテンツ情報に共通の、チャネル受信契約情  
報と、個々のコンテンツ情報に対応して放送される、複  
数の契約者に共通の、チャネル送信契約情報とを統合し  
て、指定されたコンテンツ情報に対応する利用可能契約  
情報リストを作成し、作成された利用可能契約情報リス  
トに基づいて、コンテンツ利用条件を決定し、決定され  
たコンテンツ利用条件に基づいて、受信されたコンテン  
ツ情報の利用を制御する。



1

## 【特許請求の範囲】

【請求項 1】チャンネルを用いて放送配信されるコンテンツ情報を受信する手段と、

複数のコンテンツ情報を含むチャンネルに対応して放送された、個々の契約者に対する第 1 の利用条件情報と、個々のコンテンツ情報に対応して放送された、複数の契約者に共通の第 2 の利用条件情報とを統合して、指定されたコンテンツ情報に対応する第 3 の利用条件情報を作成する手段と、

作成された前記第 3 の利用条件情報に基づいて決定されたコンテンツ利用条件に従って、受信された対応する前記コンテンツ情報の利用を制御する手段とを備えたことを特徴とする放送受信装置。

【請求項 2】前記制御する手段は、決定された前記コンテンツ利用条件に基づいてコンテンツ情報の 2 次利用に対する制御を行う手段を含むことを特徴とする請求項 1 に記載の放送受信装置。

【請求項 3】前記制御する手段は、

前記コンテンツ情報を 2 次利用する 2 次利用装置がその利用制御の際に従うべき条件を規定したライセンス情報を、決定された前記コンテンツ利用条件に基づいて作成する手段と、

前記コンテンツ情報を暗号化する手段と、

暗号化された前記コンテンツ情報を復号するための鍵と、前記ライセンス情報とを一体化して暗号化する手段と、

暗号化された前記コンテンツ情報と、暗号化された前記鍵および前記ライセンス情報とを、前記 2 次利用装置に送信する手段とを含むことを特徴とする請求項 1 に記載の放送受信装置。

【請求項 4】前記制御する手段は、前記第 3 の利用条件情報として複数のコンテンツ利用条件が作成された場合に、各コンテンツ利用条件に含まれる制限項目毎に予め定められた優先順位に従って、該第 3 の利用条件情報に含まれるコンテンツ利用条件と、入力されたユーザ所望のコンテンツ利用条件とを比較することによって、該第 3 の利用条件情報に含まれるコンテンツ利用条件を 1 つに定める手段を含むことを特徴とする請求項 1 ないし 3 のいずれか 1 項に記載の放送受信装置。

【請求項 5】前記制御する手段は、前記第 3 の利用条件情報として複数のコンテンツ利用条件が作成された場合に、予め定められた評価関数に従い、入力されたユーザ所望のコンテンツ利用条件を基準とし、該第 3 の利用条件情報に含まれるコンテンツ利用条件の各々を評価することによって、該第 3 の利用条件情報に含まれるコンテンツ利用条件を 1 つに定める手段を含むことを特徴とする請求項 1 ないし 3 のいずれか 1 項に記載の放送受信装置。

【請求項 6】前記制御する手段は、前記第 3 の利用条件情報として複数のコンテンツ利用条件が作成された場合

2

に、該複数のコンテンツ利用条件を提示し、ユーザからの選択指定を受け付けることにより、該第 3 の利用条件情報に含まれるコンテンツ利用条件を 1 つに定める手段を含むことを特徴とする請求項 1 ないし 3 のいずれか 1 項に記載の放送受信装置。

【請求項 7】前記制御する手段は、前記第 3 の利用条件情報に含まれるコンテンツ利用条件のうちに、入力されたユーザ所望のコンテンツ利用条件を包含するものが存在する場合には、該ユーザ所望のコンテンツ利用条件を採用することを決定し、該ユーザ所望のコンテンツ利用条件を包含するものが存在しない場合には、該ユーザ所望のコンテンツ利用条件を該前記第 3 の利用条件情報に適合するように修正したものを採用することを決定することを特徴とする請求項 1 ないし 6 のいずれか 1 項に記載の放送受信装置。

【請求項 8】前記コンテンツ利用条件の利用制限項目として、有効期限に関する条件、利用回数に関する条件、および機器または機種に関する条件の少なくとも 1 つを含むことを特徴とする請求項 1 ないし 7 のいずれか 1 項に記載の放送受信装置。

【請求項 9】前記制御する手段は、前記コンテンツ情報を 2 次利用装置に送信する場合に、該 2 次利用装置に対する認証を行なう手段を含むことを特徴とする請求項 1 ないし 8 のいずれか 1 項に記載の放送受信装置。

【請求項 10】前記第 2 の利用条件情報は、対応するコンテンツ情報と同一のパケットに含まれて放送されることを特徴とする請求項 1 ないし 9 に記載の放送受信装置。

【請求項 11】前記第 2 の利用条件情報は、対応するコンテンツ情報に対する電子番組ガイド情報と同一のパケットに含まれて放送されることを特徴とする請求項 1 ないし 9 に記載の放送受信装置。

【請求項 12】前記制御する手段によるコンテンツ利用条件の決定を、録画予約時に行うことを特徴とする請求項 11 に記載の放送受信装置。

【請求項 13】放送配信されるコンテンツ情報の利用を利用条件に応じて制御するコンテンツ利用制御方法であって、個々の契約者に対応して放送される、同じチャンネルに含まれる複数のコンテンツ情報に共通の、第 1 の利用条件情報と、個々のコンテンツ情報に対応して放送される、複数の契約者に共通の、第 2 の利用条件情報とを統合して、指定されたコンテンツ情報に対する利用条件を定め、定められた前記利用条件に基づいて、対応する前記コンテンツ情報の利用を制御することを特徴とするコンテンツ利用制御方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、暗号化（スクランブル）されて放送配信されるコンテンツを契約内容（例えば、期間、視聴チャンネル、録画録音の可否）に応じて



3

復号（デスクランブル）し利用あるいは2次利用する有料放送サービスのための契約受信装置及びコンテンツ利用制御方法に関する。

【0002】

【従来の技術】デジタル放送は、通信衛星（CS）に始まって、ケーブルTV、地上放送へとデジタル化が進むにつれ、一層のサービスの充実が期待されており、これから放送サービスの主役を務めていくものと思われる。

【0003】デジタル放送の最大の特徴は、情報圧縮技術の導入により、番組の送信に要する周波数の使用効率の向上が図れ、アナログ放送に比較して放送チャンネル数の大幅な増加が可能となったことである。さらに、高度な誤り訂正技術が適用できるため、高品質で均質なサービスの提供が可能となる。

【0004】また、放送のデジタル化により、従来のように画像や音声による放送だけでなく、文字やデータによる放送（データ放送）も可能になり、例えばニュースを文字データとして流すことや、PCソフトを放送で配信することが可能となり、そのようなサービスを提供するためのシステムも続々と登場してきている。

【0005】このようなシステムで、契約内容に基づいてスクランブルを解く、あるいは復号する有料放送サービスを提供する際、契約期間に即した顧客管理が行えなければならない。契約期間に即した顧客管理とは、例えば、所定の料金の支払により契約された契約期間内に限って契約チャンネルの番組の視聴を可能とするというものである。

【0006】また、受信装置にてスクランブルあるいは暗号を解くための鍵情報は、不正視聴を防止する上からも正当な視聴者のみに（契約チャンネル、契約期間に即して）しかも確実に提供する必要がある。

【0007】この意味で、従来は、図5に示すような鍵構成を用いて限定受信を行っていた。すなわち、放送受信装置毎にマスター鍵KMを用意し、受信契約している視聴者に対して受信契約しているチャンネルのワーク鍵Kwと受信契約情報をマスター鍵KMで暗号化して送信する。ここで、ワーク鍵はチャンネル固有の鍵であり、受信契約情報は当該チャンネルの契約期間あるいは契約の有無などの情報である。受信契約情報は、コンテンツ受信に先だって受信し、蓄積される。コンテンツ視聴時は、当該受信契約に関する情報を参照して、当該チャンネルの視聴可否によって、ワーク鍵を使って暗号化されて送られてくる当該チャンネルのチャンネルキーKchを復号して視聴する。チャンネルキーは、スクランブルされた放送コンテンツをデスクランブルするのに用いられる。

【0008】このように従来のデジタル放送方式では、有料放送を実現する手段として受信契約情報を用いていた。これによって、チャンネル毎の契約管理を確実に行うことができ、デジタル放送が事業として成立している。

4

しかしながら、チャンネル毎の受信契約しかサポートできず、同一チャンネル内に存在するコンテンツの価値などにまで踏み込んだ視聴管理は不可能であった。これは、例えば、2次利用を前提としたPCソフトなどのデータ放送や、高付加価値な映画コンテンツの録画の際には、録画可否をチャンネル単位でしか指定できないため問題が多かった。

【0009】

【発明が解決しようとする課題】以上のように、従来の限定受信システムでは、コンテンツ毎の利用制御が困難であった。

【0010】本発明は、上記事情を考慮してなされたもので、コンテンツ毎の利用制御を可能とする放送受信装置及びコンテンツ利用制御方法を提供することを目的とする。

【0011】

【課題を解決するための手段】本発明は、放送配信されるコンテンツ情報の利用を利用条件に応じて制御するコンテンツ利用制御方法であって、個々の契約者に対応して放送される、同じチャンネルに含まれる複数のコンテンツ情報に共通の、第1の利用条件情報と、個々のコンテンツ情報に対応して放送される、複数の契約者に共通の、第2の利用条件情報とを統合して、指定されたコンテンツ情報に対する利用条件を定め、定められた前記利用条件に基づいて、対応する前記コンテンツ情報の利用を制御することを特徴とする。

【0012】本発明（請求項1）は、チャンネルを用いて放送配信されるコンテンツ情報を受信する手段と、複数のコンテンツ情報を含むチャンネルに対応して放送された、個々の契約者に対する第1の利用条件情報（例えば、チャンネル受信契約情報に含まれる1または複数のコンテンツ利用情報）と、個々のコンテンツ情報に対応して放送された、複数の契約者に共通の第2の利用条件情報（例えば、チャンネル送信契約情報に含まれる1または複数のコンテンツ利用情報）とを統合して、指定されたコンテンツ情報に対応する第3の利用条件情報（例えば、利用可能契約情報リスト）を作成する手段と、作成された前記第3の利用条件情報に基づいて決定されたコンテンツ利用条件に従って、受信された対応する前記コンテンツ情報の利用を制御する手段とを備えたことを特徴とする。

【0013】好ましくは、前記制御する手段は、決定された前記コンテンツ利用条件に基づいてコンテンツ情報の2次利用に対する制御を行う手段を含むようにしてもよい。

【0014】好ましくは、前記制御する手段は、前記コンテンツ情報を2次利用する2次利用装置がその利用制御の際に従うべき条件を規定したライセンス情報を、決定された前記コンテンツ利用条件に基づいて作成する手段と、前記コンテンツ情報を暗号化する手段と、暗号化

5

された前記コンテンツ情報を復号するための鍵と、前記ライセンス情報とを一体化して暗号化する手段と、暗号化された前記コンテンツ情報と、暗号化された前記鍵および前記ライセンス情報とを、前記2次利用装置に送信する手段と含むようにしてもよい。このようにコンテンツ情報とリンクしたライセンス情報を作成することによって、コンテンツの2次利用における利用制御を可能とする。

【0015】好ましくは、前記制御する手段は、前記第3の利用条件情報として複数のコンテンツ利用条件が作成された場合に、各コンテンツ利用条件に含まれる制限項目毎に予め定められた優先順位に従って、該第3の利用条件情報に含まれるコンテンツ利用条件と、入力されたユーザ所望のコンテンツ利用条件とを比較することによって、該第3の利用条件情報に含まれるコンテンツ利用条件を1つに定める手段を含むようにしてもよい。

【0016】好ましくは、前記制御する手段は、前記第3の利用条件情報として複数のコンテンツ利用条件が作成された場合に、予め定められた評価関数に従い、入力されたユーザ所望のコンテンツ利用条件を基準とし、該第3の利用条件情報に含まれるコンテンツ利用条件の各々を評価することによって、該第3の利用条件情報に含まれるコンテンツ利用条件を1つに定める手段を含むようにしてもよい。この場合に、好ましくは、前記第3の利用条件情報として複数のコンテンツ利用条件が作成された場合に、予め定められた評価関数による評価値に基づいた順番で該複数のコンテンツ利用条件を表示し、ユーザに選択などをさせるようにしてもよい。

【0017】好ましくは、前記制御する手段は、前記第3の利用条件情報として複数のコンテンツ利用条件が作成された場合に、該複数のコンテンツ利用条件を提示し、ユーザからの選択指定を受け付けることにより、該第3の利用条件情報に含まれるコンテンツ利用条件を1つに定める手段を含むようにしてもよい。

【0018】好ましくは、前記制御する手段は、前記第3の利用条件情報に含まれるコンテンツ利用条件のうちに、入力されたユーザ所望のコンテンツ利用条件を包含するものが存在する場合には、該ユーザ所望のコンテンツ利用条件を採用することを決定し、該ユーザ所望のコンテンツ利用条件を包含するものが存在しない場合には、該ユーザ所望のコンテンツ利用条件を該前記第3の利用条件情報に適合するように修正したものを採用することを決定するようにしてもよい。

【0019】好ましくは、決定されたコンテンツ利用条件を表示してユーザに通知するようにしてもよい。

【0020】好ましくは、前記コンテンツ利用条件の利用制限項目として、有効期限に関する条件、利用回数に関する条件、および機器または機種に関する条件の少なくとも1つを含むようにしてもよい。

【0021】好ましくは、前記制御する手段は、前記コ

6

ンテンツ情報を2次利用装置に送信する場合に、該2次利用装置に対する認証を行なう手段を含むようにしてもよい。あるいは、放送受信装置と2次利用装置との間で相互認証を行なうようにしてもよい。

【0022】好ましくは、前記第2の利用条件情報は、対応するコンテンツ情報と同一のパケットに含まれて放送されるようにしてもよい。

【0023】好ましくは、前記第2の利用条件情報は、対応するコンテンツ情報に対する電子番組ガイド情報と同一のパケットに含まれて放送されるようにしてもよい。

【0024】好ましくは、前記制御する手段によるコンテンツ利用条件の決定を、録画予約時に行うようにしてもよい。

【0025】本発明（請求項13）は、放送配信されるコンテンツ情報の利用を利用条件に応じて制御するコンテンツ利用制御方法であって、個々の契約者に対応して放送される、同じチャネルに含まれる複数のコンテンツ情報に共通の、第1の利用条件情報と、個々のコンテンツ情報に対応して放送される、複数の契約者に共通の、第2の利用条件情報とを統合して、指定されたコンテンツ情報に対する利用条件を定め、定められた前記利用条件に基づいて、対応する前記コンテンツ情報の利用を制御することを特徴とする。

【0026】なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

【0027】本発明によれば、あるチャネルに対して契約者が持っている1または複数の第1の利用条件と、あるコンテンツに対して規定されている1または複数の第2の利用条件とを統合することによって、契約者とコンテンツのペア毎に様々な限定受信を実現することができる。このことにより、コンテンツの価値などに応じてコンテンツ毎に利用制御することが可能になり、また、従来は十分にできていなかったコンテンツの2次利用などへも限定受信を拡張することができる。

【0028】また、コンテンツ利用条件をライセンス情報という形でコンテンツとリンクさせて2次利用装置に与えることによって、コンテンツを2次利用装置に利用させることが可能になる。

【0029】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。

【0030】最初に、基本的事項の説明や語句の定義等を行なう。

【0031】放送受信装置のコントロールが直接的には及ばない機器・装置（2次利用装置と呼ぶ）でのコンテンツの利用を「2次利用」と呼ぶ。2次利用以外のコンテンツの利用を「標準利用」と呼ぶ。例えば、録画装置やPC等の外部装置は2次利用の制御の対象になるが、

7

放送受信装置と一体化されて放送受信装置のコントロールが直接及ぶテレビ出力装置やスピーカのような機器・装置（標準利用装置と呼ぶ）は2次利用の制御の対象にはない（もちろん、同種のテレビ出力装置やスピーカであっても放送受信装置のコントロールが直接的には及ばなければ2次利用装置になる）。

【0032】本実施形態では、放送受信装置が行う限定受信として、標準利用装置に関する制御（例えば、放送中のコンテンツの即時的な視聴の可否に対するチャンネル受信契約に基づく制御）と、2次利用装置での適正なコンテンツの利用を可能にするための制御を例として取り上げている。

【0033】本実施形態では、個々のユーザが番組提供側（例えば放送局）との間で基本的にはチャンネル単位で受信契約する場合を想定している。また、基本的にはユーザ毎かつチャンネル毎に契約内容（例えば利用条件）が設定される場合を想定している。少なくとも1つのチャンネルの受信契約をしたユーザ側には、限定受信を行う放送受信装置が設置される。各放送受信装置には固有の識別子（受信装置IDと呼ぶ）が付され、放送受信装置はこの「受信装置ID」により管理される。

【0034】或るチャンネルの契約状態（例えば、契約の有無、利用条件など）を示す情報を「チャンネル契約情報」と呼ぶ。チャンネル契約情報は、限定受信を行なうために放送局側から放送受信装置側に放送される制御情報である（適正な放送受信装置は、制御情報に従って限定受信のための制御を行う）。本実施形態では、本来のチャンネル受信契約によつて設定される（コンテンツ依存性のない）「チャンネル受信契約情報」と、コンテンツの価値や個性などに応じて送信側の意図によつて設定される（コンテンツ依存性のある）「チャンネル送信契約情報」の2種類のチャンネル契約情報を用いる。チャンネル受信契約情報は、例えば、契約者毎かつチャンネル毎に設定され（1つのチャンネルに含まれるコンテンツに共通に設定され）、チャンネル送信契約情報は、例えば、チャンネル毎かつコンテンツ毎に設定される（契約者に共通に設定される）。

【0035】ところで、契約状態を契約の有無のみとして考えた場合、例えば、各チャンネルにチャンネル番号を付け、図2のようにチャンネル番号に対応したビットが1であるか否かによりチャンネルの契約の有無を表したビット列が、チャンネル契約情報の一形態である。このように各チャンネル毎にその契約の有無を表記した情報をチャンネル展開情報と呼ぶ。全チャンネルでnチャンネルあるならば、チャンネル展開情報はnビットのデータとなる。図2の例では、全8チャンネルのうち、第2、第5、第7、第8チャンネルが契約済みであり、第1、第3、第4、第6チャンネルが未契約であることを示している。

【0036】ここで、特定のチャンネルに対応する、そのチャンネルの契約状態を示すビット情報を「契約フラグ」

8

と呼ぶ。例えば、図2のチャンネル契約情報においては、第1チャンネルの契約フラグは0、第2チャンネルの契約フラグは1である。

【0037】放送受信装置内において記憶されている契約フラグは、対応するチャンネルの契約の有無を表すことになるが、放送局から放送する情報の中に含める契約フラグは、対応するチャンネルが新規契約されたこと（放送受信装置内において記憶されている契約フラグを0から1へ更新させる場合）、対応するチャンネルの契約が解除されたこと（放送受信装置内において記憶されている契約フラグを1から0へ更新させる場合）、対応するチャンネルの契約の有無の確認（契約フラグが変化しない場合）などを通知するために使用できる。

【0038】チャンネルおよび契約フラグの通知（放送）の方法には、上記のチャンネル展開情報を用いる方法の他に、種々の方法がある。例えば、図3のように、チャンネル識別子とその契約フラグの組を用いて、チャンネル契約情報を個別に通知する方法がある。この場合には、必要なチャンネル（例えば、新規契約されたチャンネル、契約解除されたチャンネル、確認等のために契約状態を通知するチャンネル等）についてだけ放送するようにすることができる。また、図3において、チャンネル識別子を複数列挙して、複数のチャンネルの契約状態を取り纏めて通知する方法もある。あるいは、複数のチャンネル識別子の組を示すパッケージ識別子を用いて、複数のチャンネルの契約状態を取り纏めて通知する（あるパッケージ識別子に含まれる複数のチャンネル識別子の組を示す情報は別途放送する）方法もある。本発明はどのような形態にも適用可能であるが、本実施形態では図3に示す方法を用いる場合を例にとつて説明する。

【0039】また、本実施形態では、契約状態として、チャンネル毎の契約の有無だけではなく、より高度な限定受信の実現のために、チャンネルに関する契約内容（例えば利用条件）およびコンテンツに関する契約内容（例えば利用条件）を用いる。このために、チャンネル受信契約情報／チャンネル送信契約情報には、契約フラグの他に、契約内容に関する情報、例えば図4に示すコンテンツ利用情報が含まれる（なお、チャンネル送信契約情報では、契約フラグを設けない構成を採用してもよい）。コンテンツ利用情報は、例えば、図4に示すように有効期限情報、回数制限情報、機器限定情報を含む。

【0040】チャンネル契約情報の改ざんを防ぐ目的で、チャンネル契約情報は、暗号化されて放送配信される。また、不利なチャンネル契約情報の不取得（例えば契約解除のために放送配信されるチャンネル契約情報の不受信もしくは廃棄等）を防ぐ目的で、チャンネル契約情報を、他の情報とセットにして暗号化することもできる（この結果、それらはセットで放送される）。

【0041】本実施形態では、チャンネル受信契約情報を含む情報を（その一部または全部が暗号化されているか

否かにかかわらず)「受信契約関連情報」と呼ぶ。なお、チャンネル受信契約情報は、それが適用される放送受信機の受信装置IDと一体のものであるので、受信契約関連情報には該受信装置IDも含まれる。また、チャンネル送信契約情報を含む情報を(その一部または全部が暗号化されているか否かにかかわらず)「番組関連情報」と呼ぶ。

【0042】なお、暗号化されて放送されるコンテンツを復号するために必要なチャンネルキーは、第1の実施形態では、番組関連情報に含めて(チャンネル送信契約情報とともに暗号化されて)放送され、第2の実施形態では、受信契約関連情報に含めて(チャンネル受信契約情報とともに暗号化されて)放送される。また、第2の実施形態では、チャンネル送信契約情報はコンテンツに付加して(コンテンツとともに暗号化されて)放送される。すなわち、第2の実施形態では、番組関連情報は使用しない。

【0043】放送受信装置内部で限定受信の仕組みを実現するハードウェアを「限定受信チップ」と呼ぶ。限定受信チップは、限定受信のための秘密情報をその内部に含むことになるので、その内部のメモリやハード構成に関して外部から容易に読み出し、書き込み、変更ができないように、一体化したLSIとして構成し、耐タンパ構造を有することを仮定している。限定受信チップ内部のメモリには、マスター鍵および機器マスター鍵が含まれているものとする。マスター鍵は、主にチャンネル受信契約情報を復号するために用いられる。マスター鍵は、第1の実施形態では、放送受信装置に固有とし、第2の実施形態では、全放送受信装置に共通としている。機器マスター鍵は、放送受信装置と2次利用装置との間で共有される鍵で(各2次利用装置が機種毎に定められた機器マスター鍵を有する形態や、全ての2次利用装置が共通の機器マスター鍵を有する形態などが考えられる)、放送受信装置から2次利用装置に転送するコンテンツを暗号化するために用いられる。また、受信装置IDは、受信装置毎個別に設定され、限定受信チップ内部の不揮発性メモリの中に記録されているものとする。

【0044】本実施形態の放送受信装置で受信されるチャンネルは、「通常チャンネル」と「契約情報チャンネル」に大別することができる。通常チャンネルには通常の放送コンテンツを載せたパケットが多重化されて流されている。契約情報チャンネルには、受信契約関連情報を載せたパケットや、番組関連情報を載せたパケットが流れている。なお、契約情報チャンネルでは、各情報はそれが変更されたときにだけ放送されるのではなく、同じ内容の情報が、例えば一定期間、繰り返し放送される。本実施形態の放送受信装置は、その動作中において、上記のような契約情報チャンネルと1つ以上の通常チャンネルを常時受信するものである。

【0045】(第1の実施形態)本実施形態では、各放

送受信装置が個別のマスター鍵を有する方式を想定する。このような方式は、各放送受信装置に対し、定期的にしきも個別に受信契約関連情報等を暗号化して送信するので、限定受信のための情報の送信量は比較的大きいが、マスター鍵が破られた際の被害範囲が狭いなど、安全性が非常に高い(このような方式は、CS放送その他で採用されてきている)。

【0046】以下、本実施形態の放送受信装置について説明する。

【0047】図1に、本実施形態に係る放送受信装置の構成例を示す。

【0048】図1に示されるように、本放送受信装置は、受信部101、A/D変換部102、誤り検出/訂正部103、チャンネル選択部104、チャンネル選択インタフェース(I/F)105、限定受信処理部(限定受信チップ)106、コンテンツ利用法選択インタフェース(I/F)107、コンテンツ利用条件表示部108を有する。また、限定受信処理部100すなわち限定受信チップには、フィルタ部111、デスクランブル部112、番組関連情報復号部113、受信契約関連情報認証部114、受信契約関連情報復号部115、受信契約判定部116、利用条件判定/修正部117、コンテンツ出力制御部118、チャンネル情報入力部119、標準出力部120、2次利用出力部121、マスター鍵格納部122、受信装置ID格納部123、ワーク鍵格納部124、チャンネルキー格納部125、チャンネルキー出力部126、受信契約情報格納部127、送信契約情報格納部128が作り込まれ、耐タンパ性が付与されている。

【0049】次に、本実施形態の暗号化機構について説明する。

【0050】本実施形態の放送コンテンツは、図5に示すように、3段の暗号化機構によって保護される。

【0051】まず、上記のように、各放送受信装置は固有のマスター鍵 $K_M$ を持つ。

【0052】ワーク鍵 $K_w$ は、チャンネル毎に定められる、全ての放送受信装置に共通の鍵である。あるチャンネルに対応するワーク鍵 $K_w$ は、送信対象となる放送受信装置に固有のマスター鍵 $K_M$ でワーク鍵識別子とともに暗号化され、対応するチャンネル識別子および対象となる受信装置IDとともに送信される。あるいは、マスター鍵 $K_M$ でワーク鍵識別子および対応するチャンネル識別子とともに暗号化され、対象となる受信装置IDとともに送信されるようにしてもよい。この結果、送信すべき暗号化ワーク鍵は、放送受信装置毎かつそのチャンネル毎に存在する。各放送受信装置では、自装置のマスター鍵 $K_M$ を用いて暗号化されたワーク鍵 $K_w$ を復号し、ワーク鍵識別子およびチャンネル識別子と対応付けて記憶する。

【0053】チャンネルキー $K_{ch}$ は、スクランブル(暗号化)された放送コンテンツをデスクランブル(復号)

するための鍵であり、チャンネル毎に定められる。チャンネルキー $K_{ch}$ は、対応するワーク鍵 $K_w$ でチャンネルキー識別子とともに暗号化され、ワーク鍵識別子、および対応するチャンネル識別子とともに放送配信される。各放送受信装置では、対応するワーク鍵 $K_w$ を用いて暗号化されたチャンネルキー $K_{ch}$ を復号し、チャンネルキー識別子およびチャンネル識別子と対応付けて記憶する。

【0054】放送コンテンツは、チャンネルキー $K_{ch}$ を使って主に共有鍵暗号方式で暗号化され、チャンネルキー識別子およびチャンネル識別子とともに放送配信される。

【0055】各放送受信装置では、対応するチャンネルキー $K_{ch}$ を用いて、該放送コンテンツを復号することができる。

【0056】ここで、チャンネルキーは解読を防ぐために例えば10分程度の短時間で変更するのが望ましい。これを送信するために、個別のマスター鍵を使っていたのでは送信量が膨大となるので、全放送受信装置に共通のワーク鍵を使って送信量を削減している。一方、ワーク鍵も何ヵ月という単位で同じ鍵を使うと危険であるので、例えば1ヶ月という単位で変更するのが望ましく、これを個別のマスター鍵で暗号化して送信する。この仕組みによって、たとえマスター鍵が知られても、ワーク鍵を変更することによって無料視聴を防止することができる。

【0057】なお、ワーク鍵の配信については、例えば、チャンネル受信契約情報に含めて配信する形態、ワーク鍵パケットで配信する形態などが考えられる（本実施形態では、チャンネル受信契約情報に含めて配信するものとする）。

【0058】以下、この限定受信システム上でチャンネル受信契約情報とチャンネル送信契約情報とを統合することにより詳細な限定受信を実現する例を示す。ここでは、限定受信の詳細な例として、コンテンツ2次利用の限定受信による制御方式を取り上げる。もちろん、2次利用での利用制限を目的とした限定受信は一例であり、コンテンツ毎に異なる利用形態を定めなくてはならないようなシステムにおいては、同様の方式を使用することができる。

【0059】ところで、コンテンツの2次利用は記録メディアに記録しておくことにより何度でも利用できるように利用形態を含むので、その利用形態はコンテンツの価値などに深く依存する。その意味で、従来の受信契約情報のみによる限定受信であるとチャンネル毎にしか管理できないので、例えば、チャンネルに様々な価値のコンテンツが流れる場合、それらの価値を反映させた個別の制御ができなかった。この問題は、特に録画装置などの外部装置へ出力する際に顕著であり、従来は、一律にコピープロテクションをかけるか、無制限に2次利用を認めるかのどちらかしかなく、例えばコピープロテクションがかかっているチャンネルを相当の対価を払って録画可能

にするような限定受信は存在しなかった。また、今後デジタル放送事業が拡大してデータ放送が事業化され、それに伴って2次利用形態が高度化し、デジタル録画が可能になったり、配信ソフトのPCでの実行が可能となってきたような場合には、この問題はより深刻になる。本実施形態では、この問題を、契約者の持つチャンネル受信契約情報とコンテンツの持つチャンネル送信契約情報を統合することにより実現しようとするものである。

【0060】まず、チャンネル契約情報（チャンネル受信契約情報／チャンネル送信契約情報）について説明する。

【0061】本限定受信システムによりコンテンツの2次利用を制御する場合、チャンネル受信契約情報（あるいはそれが示す契約状態）には、そのチャンネルの契約の有無と、契約ありの場合における、そのチャンネルで放送されるコンテンツの利用に対する利用条件（制限内容）と当該チャンネルのワーク鍵 $K_w$ （ワーク鍵をチャンネル受信契約情報に含めて配送する場合）を含む。また、チャンネル送信契約情報（あるいはそれが示す契約状態）は、そのコンテンツの利用に対する利用条件を含む。

【0062】図3に、本実施形態のチャンネル契約情報のデータ構造例を示す。（a）が、ワーク鍵をチャンネル受信契約情報に含めて配送する場合におけるチャンネル受信契約情報であり、（b）がチャンネル送信契約情報と、ワーク鍵をチャンネル受信契約情報に含めて配送しない場合におけるチャンネル受信契約情報である。

【0063】図3（a）のチャンネル受信契約情報は、チャンネル識別子、契約フラグ、ワーク鍵識別子、ワーク鍵、コンテンツ利用形態数、コンテンツ利用形態数だけのコンテンツ利用情報の列からなる。

【0064】「チャンネル識別子」は、当該放送コンテンツがどのチャンネルのコンテンツかを示すものである。

【0065】「契約フラグ」は、チャンネル識別子で指定されているチャンネルの契約状態を示すビット情報である。

【0066】「ワーク鍵識別子」は、ここで配信するワーク鍵の識別子である。

【0067】「ワーク鍵」は、当該チャンネルのワーク鍵 $K_w$ である。

【0068】「コンテンツ利用形態数」は、本チャンネル契約情報に含まれるコンテンツ利用情報の数を示す。

【0069】「コンテンツ利用情報」は、コンテンツに対する利用条件に関する情報を示す。

【0070】なお、契約フラグが1の場合にワーク鍵識別子のフィールドおよびワーク鍵のフィールドを有効としてもよいし（契約フラグが0の場合にも、図3（a）のようになる）、契約フラグが1の場合にそれらフィールドをチャンネル受信契約情報に含めるようにしてもよい（契約フラグが0の場合には、図3（b）のようになる）。

【0071】なお、以下では、ワーク鍵に関する説明は

省略する。

【0072】コンテンツ利用情報は、本実施形態では図4に示すように、「有効期限情報」、「回数制限情報」、「機器制限情報」からなるものとする。「有効期限情報」、「回数制限情報」、「機器制限情報」は、それぞれ、当該コンテンツが利用できる、時間的期限、回数的制限、利用される機器の限定を意味し、全て固定長で予め定められた形式で記述されている。

【0073】図3(b)のチャンネル送信契約情報またはチャンネル受信契約情報は、チャンネル識別子、契約フラグ、コンテンツ利用形態数、コンテンツ利用形態数だけのコンテンツ利用情報の列からなる。各情報は、上記の通りである。

【0074】次に、放送される各種データについて説明する。

【0075】本実施形態の限定受信システムにおいて放送受信装置が受信するデータのうちには、コンテンツパケット、番組関連情報パケット、受信契約関連情報パケットがある。

【0076】まず、放送コンテンツについて説明する。

【0077】図6に、コンテンツパケットのデータ構造例を示す。

【0078】コンテンツパケットは、図6に示すように、情報識別子、チャンネル識別子、チャンネルキー識別子、放送コンテンツからなっている。

【0079】「情報識別子」は、当該パケットの種別を示すもので、ここではコンテンツパケットであることを示す識別子を記述する。

【0080】「チャンネル識別子」は、当該放送コンテンツがどのチャンネルのコンテンツかを示すものである。

【0081】「チャンネルキー識別子」は、当該放送コンテンツを復号するためのチャンネルキーの識別子を示す。

【0082】「放送コンテンツ」は、生の番組データで、チャンネルキー識別子で指定されたチャンネルキーK<sub>ch</sub>で暗号化されている。

【0083】なお、本実施形態ではこれら全ての情報は固定長で表現されたデータであるとする。

【0084】次に、番組関連情報について説明する。

【0085】図7に、番組関連情報パケットのデータ構造例を示す。

【0086】番組関連情報パケットは、図7に示すように、情報識別子、チャンネル識別子、ワーク鍵識別子、チャンネルキー識別子、チャンネルキー、チャンネル送信契約情報からなっている。

【0087】「情報識別子」は、当該パケットの種別を示すもので、ここでは番組関連情報パケットであることを示す識別子を記述する。

【0088】「チャンネル識別子」は、当該番組関連情報がどのチャンネルのものかを示すものである。

【0089】「ワーク鍵識別子」は、当該番組関連情報

パケットがどのワーク鍵K<sub>w</sub>によって暗号化されているかを示す情報である。

【0090】「チャンネルキー識別子」は、次に記述されているチャンネルキーの識別子である。

【0091】「チャンネルキー」は、チャンネル識別子で指定されているチャンネルの放送コンテンツの暗号化に使われているチャンネルキーK<sub>ch</sub>を示している。

【0092】「チャンネル送信契約情報(C<sub>s</sub>)」は、上記チャンネルキーK<sub>ch</sub>で暗号化されているコンテンツの利用条件を記述したチャンネル契約情報である。

【0093】なお、本実施形態では、これら全ての情報は固定長で表現されたデータであり、チャンネルキー識別子、チャンネルキー、およびチャンネル送信契約情報の範囲がワーク鍵識別子で指定されたワーク鍵で暗号化されている。

【0094】ここで、本実施形態では、同時刻に放送されているコンテンツと、番組関連情報とが対応するものとする(番組関連情報の放送の開始が、対応するコンテンツの放送の開始に若干先行し、番組関連情報の放送と、対応するコンテンツの放送が同時に終了する場合、番組関連情報の放送の開始および終了が、対応するコンテンツの放送の開始および終了に若干先行する場合、などを含む)。なお、その代わりに、各パケットにコンテンツ識別子を付加して、明示的に対応を取るようにしてもよい。

【0095】次に、受信契約関連情報について説明する。

【0096】図8に、受信契約関連情報パケットのデータ構造例を示す。

【0097】受信契約関連情報パケットは、図8に示すように、情報識別子、受信装置ID、チャンネル受信契約情報、誤り検出コードからなっている。

【0098】「情報識別子」は、当該パケットの種別を示すもので、ここでは受信契約関連情報パケットであることを示す識別子を記述する。

【0099】「受信装置ID」は、当該受信契約関連情報がどの放送受信装置宛てのものかを示すものである。

【0100】「チャンネル受信契約情報(C<sub>R</sub>)」は、当該放送受信装置の契約状態を示すチャンネル契約情報である。

【0101】「誤り検出コード」は、チャンネル受信契約情報の誤りを検出するコードである。

【0102】なお、本実施形態ではこれら全ての情報は固定長で表現されたデータであり(ただし、前述のように、チャンネル受信契約情報が可変になる形態もある)、チャンネル受信契約情報から誤り検出コードまでが受信装置IDの示す受信装置のマスター鍵で暗号化されている。

【0103】以下、本実施形態の放送受信装置の動作について説明する。

【0104】図9～図12に、本実施形態の放送受信装置の動作手順の一例を示す。

【0105】まず、ユーザの操作により手動的にもしくは予約機能等により自動的に、チャンネル選択インターフェース105で所望のチャンネルが選択されるものとする。チャンネル選択インターフェース105で選択されているチャンネル番号は、チャンネル選択部104へ伝えられ、またチャンネル情報入力部119から受信契約判定部116へ伝えられる。

【0106】さて、図9のステップS11において受信部101で受信された放送波は、A/D変換部102でA/D変換を施されてデジタルデータにされ（ステップS12）、当該放送受信装置内部で処理可能なパケットに再構築される。そして、誤り検出／訂正部103で誤り検出／訂正される（ステップS13）。

【0107】誤り検出／訂正された受信パケットはチャンネル選択部104に送られ、放送コンテンツパケット（図6）については、チャンネル選択インターフェース105にて選択されたチャンネルに対応するもののみが、そして、番組関連情報パケット（図7）および受信契約関連情報パケット（図8）については全パケットが、限定受信処理部100に送られる。

【0108】以降は、パケットの種別に応じて処理が分岐する。

【0109】フィルター部111では、受信パケットの情報識別子を参照し、コンテンツパケットである場合は（ステップS14）、これをデスクランブル部112へ送る（ステップS17、S18）。コンテンツパケットを与えられたデスクランブル部112では、暗号化コンテンツの復号化のための処理を開始する。

【0110】番組関連情報パケットである場合は（ステップS15）、番組関連情報復号部113へ送る（ステップS19）。番組関連情報パケットを与えられた番組関連情報復号部113では、チャンネルキーおよびチャンネル送信契約情報の復号化のための処理を開始する。

【0111】受信契約関連情報パケットである場合は（ステップS16）、受信契約関連情報認証部114へ送る（ステップS20）。すなわち、この受信契約関連情報パケットには受信装置個別のマスター鍵によって暗号化されている部分があるので、復号に先だって自装置宛てのパケットであるか否かを判定する。受信契約関連情報パケットを与えられた受信契約関連情報認証部114では、パケット内に含まれる受信装置IDを抽出し、受信装置ID格納部123から取り出した受信装置IDと比較することにより、当該受信契約情報パケットが自装置宛てのものかどうかを判定し、自装置宛ての受信契約情報であれば、受信契約関連情報復号部115へ送り、そうでなければ処理を終了する。自装置宛ての受信契約関連情報パケットを与えられた受信契約関連情報復号部115では、チャンネル契約情報の復号化のための処

理を開始する。

【0112】次に、コンテンツパケットに関する処理について説明する。

【0113】受信コンテンツパケットを受け取ったデスクランブル部112では、図10に例示したような手順で処理を行う。

【0114】フィルター部111からデスクランブル部112へ送られたコンテンツパケットは、チャンネルキー出力部126に対して、チャンネル識別子およびチャンネルキー識別子を送り、チャンネルキーの出力を要請する（ステップS31）。チャンネルキー出力部126ではこの要請を受けて、受信契約判定部116に対して、チャンネル識別子を送り、チャンネルキーの出力の可否を問い合わせる（ステップS32）。受信契約判定部116ではこの問い合わせに応じて、受信契約情報格納部127から当該チャンネルの受信契約情報を引き出し（ステップS33）、契約フラグが1であれば許可、0であれば不許可を示す信号をチャンネルキー出力部126に送る（ステップS34～S37）。

【0115】チャンネルキー出力部126では、送られてきた可否の判定結果が許可であれば、チャンネルキー格納部125から当該チャンネルの当該チャンネルキー識別子を保持したチャンネルキーを得てデスクランブル部111へ送信し（ステップS38）、不許可であれば、そこで当該コンテンツパケットに関する処理を終了する。

【0116】なお、コンテンツパケットはパケットの中でも最も処理頻度が高いので、パケット毎に同様の処理を繰り返すと処理に時間がかかるため、以下の処理を行うと便利である。すなわち、同一チャンネルの同一チャンネルキーを用いている限りは一回チャンネルキーの出力許可がおりたならば、毎回受信契約判定部116に問い合わせずにチャンネルキーを出力するようにすると便利である。実際、チャンネルキーはセキュリティ上の理由で数分に1回変更されるため、このようにしても限定受信に与える影響は少ない。

【0117】チャンネルキー $K_{ch}$ の出力を受けたデスクランブル部112では、コンテンツパケットの暗号化部分を復号して（ステップS39）、コンテンツ出力制御部118へ送る（ステップS40）。

【0118】コンテンツ出力制御部118では、コンテンツ利用方法選択I/F106を介して、ユーザから入力された当該チャンネルのコンテンツ利用方法（例えば、コンテンツ利用条件や利用形態等の情報を含む）を取得し、その利用方法が可能か否かを判定する（ステップS41）。この判定は、利用条件判定／修正部117で行われる。なお、この判定処理については後に詳しく説明する。

【0119】利用条件判定／修正部117で利用許可された場合、その利用形態が標準出力（標準利用のための標準利用装置に対する出力）か2次利用出力かに従って



17

それぞれ標準出力部120、2次利用出力部121に出力される(ステップS42)。

【0120】その利用形態が標準出力である場合、標準出力部120では、当該コンテンツを標準利用装置に対して出力する(ステップS43)。

【0121】一方、その利用形態が2次利用出力である場合、2次利用出力部121では、利用形態を反映したライセンス情報を生成し(ステップS44)、ライセンス情報をコンテンツにリンクさせて2次利用装置へ出力する(ステップS45)。なお、詳しくは後述するが、  
10 コンテンツは2次利用装置との間で共有する機器マスター鍵 $K_m$ で暗号化して出力する。なお、ライセンス情報の生成処理については後に詳しく述べる。

【0122】次に、利用条件判定/修正部117の動作を図11(判定処理)、図12(修正処理)に示すフローチャートに沿って説明する。

【0123】図11は、ユーザの所望するコンテンツ利用条件を修正なしに許可できるか否かを判定する部分の処理手順の一例である。

【0124】利用条件判定/修正部117は、当該チャ  
20 ネルのコンテンツ利用条件が入力されると、受信契約情報格納部127から当該チャネルの受信契約情報を取得する(ステップS51)。

【0125】受信契約情報格納部127において、チャネル受信契約情報は、例えば図13に示すような形式で格納されている。

【0126】有効期限情報は、当該チャネルで放送されたコンテンツの利用可能な有効期限を示す。図13における有効期限情報は簡単のため「年、月、日」の形式で  
30 記述しているが、実際には一つの整数値で表されるものとする。ここで、有効期限情報が“-1”の場合は、有効期限に制限がないことを示し、有効期限情報が“0”の場合は、有効期限が無指定で、即時的にしか有効でないことを示すものとする。

【0127】回数制限は、当該チャネルで放送されたコンテンツを使用して良い回数を示す。また、上記と同様に、“-1”は無制限(何回使用しても良い)を、“0”は無指定で、即時的にしか有効でない(例えば放送時に視聴のみ可能)を示すものとする。

【0128】機器限定情報については、0が機器を限定しない、1が機器を限定する、を意味するものとする。また、それぞれのチャネル受信契約情報に指定されている有効期限情報、回数制限情報、機器限定情報は、そのAND条件で1つの契約状態を表している。例えば、  
40 図13の例において上から3番目の契約条件は2000年1月7日まで10回までどの機器でも視聴することができることを意味している。

【0129】当該チャネルのチャネル受信契約情報を取得したら、その個数を計算し、変数 $CR_{MAX}$ に格納する(ステップS52)。

18

【0130】同様に、利用条件判定/修正部117は、送信契約情報格納部128から当該チャネルの送信契約情報を取得する(ステップS53)。

【0131】送信契約情報格納部128において、チャネル送信契約情報は、例えば図14に示すような形式で格納されている。図14における各情報の意味は上記のチャネル受信契約情報と同様である。

【0132】当該チャネルのチャネル送信契約情報を取得したら、その個数を計算し、変数 $CS_{MAX}$ に格納する(ステップS53、S54)。

【0133】次に、チャネル受信契約情報を順次チェックし、入力されたコンテンツ利用条件に合致する条件を探す(ステップS55~S59)。

【0134】例えば、ユーザの所望するコンテンツ利用条件が「1999年6月9日まで回数制限なし、機器限定なし、で視聴したい」であれば、図13の例では、1番目のチャネル受信契約情報に合致する。

【0135】合致するものがあつた場合には、同様に、チャネル送信契約情報を順次チェックし、入力されたコンテンツ利用条件に合致する条件を探す(ステップS60~S64)。

【0136】そして、合致するものがあつた場合には、当該コンテンツ利用条件を許可する(ステップS65)。

【0137】すなわち、ユーザの所望するコンテンツ利用条件を満たすチャネル受信契約情報およびチャネル送信契約情報が存在すれば、当該コンテンツ利用条件を許可する旨の信号をコンテンツ出力制御部118に送信して、判定処理を終了する。

【0138】一方、チャネル受信契約情報とチャネル送信契約情報の少なくとも一方に合致するものがなかった場合には、不許可を示す信号をコンテンツ出力制御部118に送信して判定処理を終了するようにしてもよいが、本実施形態では、コンテンツ利用条件を修正して許可を出すようにしている。

【0139】例えば、上記のコンテンツ利用条件「1999年6月9日まで、回数制限なし、機器限定なし、で視聴したい」の場合には、図14の例では、合致するチャネル送信契約情報がないので、このままでは許可することができない。以下のように、利用条件を修正する処理を行う。

【0140】図12は、コンテンツ利用条件の修正が必要となつた場合の処理手順の一例である。

【0141】この場合は、まず、チャネル受信契約情報とチャネル送信契約情報とを統合して、利用可能な契約情報のリスト(以下、利用可能契約情報リスト)を作る(ステップS71)。

【0142】利用可能契約情報リストは、例えば、図13のようなチャネル受信契約情報のうちの1つのチャネル  
50 受信契約条件および図14のようなチャネル送信契約



19

情報のうちの1つのチャンネル送信契約条件について3つの個別条件毎のAND条件をとって契約条件を作成する処理を、全てのチャンネル受信契約条件とチャンネル送信契約条件との組み合わせについて行うことにより、作成される。図15に、図13に示すチャンネル受信契約情報と図14に示すチャンネル送信契約情報を統合して得た利用可能契約情報リストの一例を示す。

【0143】以下、利用可能契約情報リストの中から、ユーザが所望するコンテンツ利用条件に最も近い条件を抽出する統合処理について説明する。

【0144】ここでは、個別条件に優先順位を付け、その優先順位に従って統合されたコンテンツ利用条件に順位を付加し、最も順位の高い契約利用条件を修正利用条件とする方式を採用する。また、優先順位として、「回数制限」→「有効期限」→「機器限定」の順が設定されているものとする。すなわち、この順番で入力されたコンテンツ利用条件に適合するものを探し、最も有利と評価されるものを検索するわけである。

【0145】まず、本例では回数制限が1番目に優先されているので、回数制限から利用可能契約情報リストを参照する(ステップS72)。上記のコンテンツ利用条件「1999年6月9日まで、回数制限なし、機器限定なし」の場合には、回数制限が無制限(-1)であるため、図15に示す利用可能契約情報リストの中から回数制限が指定されていないものがあるかどうかをチェックし、ある場合にはそれらを抽出したリストを作成する(ステップS74)。図15の例では、回数制限が無制限である利用可能契約情報があるので、それらを取り出し、図16に示すようなリストを作成する。

【0146】なお、条件を満たすような利用可能契約情報がなかった場合には、利用可能契約情報リストの中で最も回数制限情報の指定数の多いものを抽出して、同様にリストを作成する(ステップS73)。

【0147】次に、本例では有効期限が2番目に優先されているので、抽出されたリストを参照し(ステップS75)、該リストの中から有効期限がコンテンツ利用条件を満たすものを抽出する(ステップS77)。図16の例の場合には、2番目の利用可能契約情報「1999年6月10日まで回数制限なし、機器限定あり」が抽出される。もちろん、複数の利用可能契約情報が抽出される場合もある。

【0148】一方、有効期限が利用条件を満たすような利用可能契約情報がなければ、抽出されたリストの中から有効期限が最も長い利用可能契約情報を抽出する(ステップS76)。

【0149】最後に、最も期間の長い契約条件を抽出し、これと入力されたコンテンツ利用条件とのANDを取ることで、修正されたコンテンツ利用条件を作成し、これをコンテンツ出力制御部118とコンテンツ利用条件表示部107に出力する(ステップS78)。

20

【0150】本例の場合、入力利用条件に最も近い(修正された)利用条件は、ユーザ所望の条件「1999年6月9日まで、回数制限なし、機器限定なし」と抽出された統合利用条件「1999年6月10日まで、回数制限なし、機器限定あり」とのANDから、「1999年6月9日まで、回数制限なし、機器限定あり」となる。すなわち、本例では、機器限定なしの条件では不許可となることを、機器限定の条件を付加する修正を行うことによって、ユーザの希望を最大限に満たした上で、許可が得られるようになっている。

【0151】コンテンツ出力制御部118に出力されたコンテンツ利用条件は、2次利用出力部121に送られ、後述する処理によって、当該コンテンツの利用方法を記述したライセンス情報に反映される。

【0152】また、コンテンツ利用条件表示部107では、入力された利用条件を表示する。本実施形態においては、希望利用条件が修正される場合があるので、ユーザへの利用条件の提示という意味で重要である。

【0153】なお、許可できる修正利用条件が得られないような場合には、例えば、不許可にして処理を終了してもよいし、あるいはユーザに希望するコンテンツ利用条件の変更を促すメッセージを表示するようにしてもよい。

【0154】このようにすることで、チャンネル受信契約情報とチャンネル送信契約情報とを統合し、当該チャンネルに対して契約者が持っているチャンネル受信契約による利用条件と個々のコンテンツに対する利用条件とを統合することことができ、契約者とコンテンツのペア毎に様々な限定受信を実現することができる。このことにより、従来は十分にできていなかったコンテンツの2次利用などへも限定受信を拡張することができる。

【0155】次に、2次利用のためのライセンス情報について説明する。

【0156】この処理は、コンテンツ利用条件を、ライセンス情報というコンテンツにリンクしたデータとして、実現するものである。

【0157】図17に、ライセンス情報の構成例を示す。

【0158】図17に例示するように、ライセンス情報は、コンテンツID、コンテンツ利用条件、コンテンツ鍵Kcからなっている。

【0159】「コンテンツID」は、2次利用出力部121内で生成される、コンテンツの識別子であり、コンテンツとライセンス情報とを形式的にリンクする役割を持つ。

【0160】「コンテンツ利用条件」は、当該コンテンツIDのついたコンテンツを利用できる条件である。本実施形態では、コンテンツ利用条件は、図18に示すように、「有効期限」、「利用回数」、「機器ID」からなるものとする。有効期限と利用回数は、チャンネル契約

21

情報と同様に、無制限を-1、無指定を0で表すものとする。また、機器IDは、0で機器限定なしを表し、0以外の値で機器限定あり表し、また、本実施形態では、0以外の機器IDは、2次利用される機器の内部に書き込まれているIDを示すものとする。

【0161】なお、先の処理で最終的に決定されたコンテンツ利用条件（ユーザが最初に入力した条件もしくは修正された条件）と、ライセンス情報におけるコンテンツ利用条件（図17、図18）とを区別するために、ライセンス情報におけるコンテンツ利用条件を2次利用条件と呼ぶものとする。

【0162】このライセンス情報における2次利用条件は、コンテンツ出力制御部118から入力されたコンテンツ利用条件をもとに生成/決定される。

【0163】「コンテンツ鍵Kc」は、コンテンツIDで指定されるコンテンツを復号するための鍵である。

【0164】ライセンス情報は、2次利用条件からコンテンツ鍵までの範囲が、機器マスター鍵Kmで暗号化されている。

【0165】次に、2次利用のためのコンテンツ情報について説明する。

【0166】図19に、コンテンツ情報の構成例を示す。

【0167】図19に示されるように、コンテンツ情報は、コンテンツIDとコンテンツからなり、コンテンツの部分のみがコンテンツ鍵Kcで暗号化されている。

【0168】ここで、コンテンツ鍵Kcは、ライセンス情報に暗号化して含まれており、これが実質的なライセンス情報とコンテンツとのリンクになっている。すなわち、ここでは機器マスター鍵Kmは2次利用装置に厳重に秘匿されており、ユーザには知られることがないと仮定している。このため、コンテンツ鍵は機器マスター鍵がなくては取得できず、コンテンツ鍵を取得できるのは2次利用装置であるため、コンテンツとライセンス情報とは「コンテンツを復号するためにはライセンス情報が必要である」という意味でリンクされている。さらに、コンテンツ鍵は、2次利用条件と一緒に暗号化されているため、2次利用条件も同様にコンテンツにリンクされるばかりか、ライセンス情報を偽造すればコンテンツ鍵も破壊されるため、実質的に2次利用条件の改竄も不可能となる。本実施形態では、このようにライセンス情報という形で、コンテンツ利用条件の2次利用への反映を行う。

【0169】さて、2次利用出力部121は、コンテンツ出力制御部118から与えられたライセンス情報およびコンテンツをもとに、2次利用のためのライセンス情報と暗号化コンテンツを作成する。

【0170】図20に、2次利用出力部121の構成例を示す。図20に示されるように、2次利用出力部121は、コンテンツ入力部201、コンテンツ暗号化部2

22

02、コンテンツ出力部203、コンテンツキー生成部204、利用条件入力部205、利用条件生成部206、コンテンツID生成部207、ライセンス情報生成部208、機器マスター鍵格納部209、ライセンス情報出力部210を含む。

【0171】まず、2次利用のためのライセンス情報作成処理について説明する。

【0172】図21に、2次利用のためのライセンス情報の作成手順の一例を示す。

【0173】まず、利用条件入力部205からコンテンツ利用条件が入力される（ステップS81）。入力されたコンテンツ利用条件は、直ちに利用条件生成部206に送られ、当該コンテンツ利用条件に対応するコンテンツのコンテンツIDとコンテンツキーKcの生成をそれぞれコンテンツID生成部207、コンテンツキー生成部204に要請し、それぞれが生成を行う（ステップS82、S83）。また、コンテンツ利用条件を参照し（ステップS84）、コンテンツ利用条件に機器限定情報がある場合には、機器IDを2次利用装置から取得する（ステップS85）。

【0174】次に、入力されたコンテンツ利用条件（および機器限定情報がある場合における機器ID）から、2次利用条件を作成する（ステップS86）。

【0175】次に、機器マスター鍵Kmを機器マスター鍵格納部209から取得し（ステップS87）、作成された2次利用条件とコンテンツキーを機器マスター鍵Kmで暗号化し、コンテンツIDを付加することにより、ライセンス情報を作成する（ステップS88）。

【0176】なお、機器マスター鍵の管理形態には、例えば、各2次利用装置が機種毎に定められた機器マスター鍵を有する形態（機器マスター鍵格納部209には、機種ID毎に対応した機器マスター鍵が格納される）、全ての2次利用装置が共通の機器マスター鍵を有する形態（共通の機器マスター鍵が格納される）などが考えられ、例えばステップS87においては上記の形態に応じて、対象となる2次利用装置の機種IDに対応する機器マスター鍵、あるいは全ての2次利用装置に共通の機器マスター鍵を取得するようにすればよい。また、例えば、各2次利用装置が個別に定められた機器マスター鍵を有するようにすることもできる。

【0177】最後に、作成されたライセンス情報を出力する（ステップS89）。

【0178】次に、コンテンツ暗号化処理について説明する。

【0179】図22に、コンテンツ暗号化の処理手順の一例を示す。

【0180】コンテンツは、コンテンツ入力部201から入力されると（ステップS91）、直ちにコンテンツ暗号化部202に送られる。コンテンツ暗号化部202は、生成されたコンテンツキーをコンテンツキー生成部

23

204から取得し（ステップS92）、コンテンツを暗号化する（ステップS93）。暗号化されたコンテンツは、コンテンツ出力部203から出力される（ステップS94）。

【0181】なお、図19の暗号化されたコンテンツおよび図17の暗号化されたライセンス情報を受信した2次利用装置では、例えば、自装置の機器マスター鍵 $K_m$ でライセンス情報を復号してコンテンツ利用条件（図18）およびコンテンツキー $K_c$ を取り出し、コンテンツ利用条件に含まれる機器IDが0または自装置の機器IDを示しており且つコンテンツ利用条件に含まれるその他の条件が満たされていることを確認した後に、暗号化されたコンテンツをコンテンツキー $K_c$ で復号し、録画や再生などの所定のコンテンツ利用を行う。2次利用装置では、コンテンツの利用にあたっては、ライセンス情報内のコンテンツ利用条件に従って、利用に対するコントロールを行う。例えば、有効期限や利用回数の管理を行う。また、コンテンツおよびそのライセンス情報を、ある2次利用装置から他の2次利用装置に転送可能としてもよい。

【0182】このようにすることにより、機器限定されていない場合、当該コンテンツは、他の2次利用機器でも利用できるようになる。

【0183】また、標準出力部120から標準利用装置にコンテンツを出力する際に、その利用がコンテンツの蓄積を伴うものである場合には、2次利用装置と同様に扱うようにしてもよい。この場合には、コンテンツ利用条件（図17）については暗号化しないで渡すようにしてもよい。また、放送受信装置と2次利用装置との間で認証手続きを行うようにする場合においても、放送受信装置と標準利用装置の間では認証を省くようにしてもよい。

【0184】このようにすることにより、契約者のチャンネル受信契約情報とコンテンツに付随するチャンネル送信契約情報とを統合し、契約者とコンテンツの利用条件の組合せで詳細な利用形態を実現することができる。また、特に本実施形態では、利用条件として2次利用での利用条件を考えてコンテンツ利用条件を作成し、そのコンテンツ利用条件をライセンス情報という形でコンテンツとリンクし、2次利用装置での利用を利用条件に制限するようなシステムを実現することができる。

【0185】さて、以下では、番組関連情報パケットに関する処理（図9のBの続き）について説明する。

【0186】図9の全体処理の流れを示したフローチャートにおいて、受信パケットが番組関連情報パケットであった場合、フィルター部111を通して、番組関連情報復号部113に送られる。

【0187】図23に、以降の処理手順の一例を示す。

【0188】この場合、まず、対応するワーク鍵を、当該パケットに付加されたチャンネル識別子およびワーク鍵

24

識別子をキーにして、ワーク鍵格納部124から取得する（ステップS101）。なお、対応するワーク鍵がワーク鍵格納部124内に存在しなかった場合は、処理を終了する。

【0189】ワーク鍵が取得できた場合には、取得したワーク鍵を使って、番組関連情報を復号する（ステップS102）。

【0190】復号された番組関連情報の中からチャンネル送信契約情報 $C_s$ を取得し（ステップS103）、これをチャンネル識別子とともに送信契約情報格納部128に格納する（ステップS104）。ここで、チャンネル送信契約情報は、放送コンテンツによって変更されるので、本実施形態では、送信契約情報格納部128において、同一のチャンネル識別子を持つチャンネル送信契約情報は常に上書きされるものとする。もちろん、全く同じ情報を上書きするのを省くために、既に存在するチャンネル送信契約情報と比較し、同一でない場合にのみ上書きするようにしてもよい。

【0191】以下では、受信契約関連情報パケットに関する処理（図9のCの続き）について説明する。

【0192】図9の全体処理の流れを示したフローチャートにおいて、受信情報が受信契約関連情報パケットであった場合、フィルター部111を通して受信契約関連情報認証部114に送られる。

【0193】図24に、以降の処理手順の一例を示す。

【0194】この場合、まず、受信装置ID格納部123から受信装置IDを抽出し（ステップS111）、これと受信契約関連情報パケットに含まれる受信装置IDとを比較することにより、当該チャンネル受信契約情報が自装置宛てのものであるか否かを判定する（ステップS112）。自装置宛てのものでなかった場合には、処理を終了する。

【0195】自受信装置のものであった場合には、放送受信装置に個別に設定されているマスター鍵 $K_M$ をマスター鍵格納部122から取得し（ステップS113）、受信契約関連情報パケットの暗号化部分を復号する（ステップS114）。

【0196】復号したチャンネル受信契約情報から誤り検出コードを取得し、その誤り検出コードを検証することにより、当該チャンネル受信契約情報が正しいものであることを確認することができる。

【0197】ここで、誤り検出コードを付加して送信し、放送受信装置側でこれを確認しているのは、受信契約関連情報パケットの中で暗号化されていない受信装置IDを偽造して偽の受信契約関連情報を作成し、入力されることを防ぐためである。誤り検出コードはチャンネル受信契約情報から導出されるものであり、チャンネル受信契約情報を暗号化したまま改変して、偽造しようとしても復号した際、得られたチャンネル受信契約情報から導出された誤り検出コードと復号の結果得られた誤り検出コ

25

ードが一致することは極めて稀であり、偽造防止を防ぐことができる。実際、誤り検出コードがないと暗号化されたチャネル受信契約情報を適当に改変することにより、復号した結果が以前よりも良い契約情報（契約内容）になっている可能性は高く、このような攻撃が容易に成功してしまう。

【0198】誤り検出コードが検証されたら（ステップS115）、受信契約関連情報パケットからワーク鍵 $K_w$ と受信契約情報 $C_R$ を取得し（ステップS116）、それぞれワーク鍵格納部124、受信契約情報格納部116に格納する（ステップS117）。

【0199】次に、本実施形態の幾つかのバリエーションについて説明する。

【0200】＜バリエーション1＞まず、コンテンツ利用情報の種類に関するバリエーションについて説明する。

【0201】以上では、図4に例示するような、有効期限、回数制限、機器制限からなるコンテンツ利用情報を想定して説明したが、もちろん、利用制限はこれらの他にも種々のものが考えられる。

【0202】その一例としては、機種制限のような利用条件が考えられる。これはコンテンツの利用をある機種に限るための条件で、例えば、当該放送コンテンツを特定機種の機器にのみに利用可能にすることによって、特定機種の売上げを促進し、そのために放送契約料金を割安にするなどの運用が可能になる。また、そのような運用以外にも、機種によっては利用条件の管理にセキュリティホールがあり、利用条件が遵守されないことも考えられる。そのような場合に、利用条件に機種制限を入れておくと、そのような機種への2次利用を制限することができる。また、機種限定を入れた場合のライセンス情報には、許可される機種の機種IDを埋め込む方法が考えられる。

【0203】また、同様に、コピー防止やコピー回数制限などを利用条件に盛り込むことも可能である。このようにすることによって、2次利用装置からのコピー回数を制限することができる。

【0204】＜バリエーション2＞次に、チャネル契約情報の記述方式に関するバリエーションについて説明する。

【0205】図4のように情報をそのまま記述する方式（展開形式）の他にも、図25のように利用条件を制限することを前提にそれをビット列で表現する方式（ビット形式）が使用可能である。図25（a）に示したチャネル受信契約情報や（b）に示したチャネル送信契約情報は、有効期限、コピー回数、機器限定が利用条件として挙がっており、それぞれ、「無制限、1週間、即時」「無制限コピー可、1回コピー可、コピー不可」、「限定なし、限定あり」の条件に制限されており、これらの組合せて表現できる18通りの条件を対応するビットが

26

1であることによって表現している。すなわち、若干18ビットのデータでチャネル契約情報を表現することができる。このような形式のチャネル契約情報を使い、利用条件を統合する際はビット毎の論理積（AND）を使うことにすれば、簡単に統合利用条件を作成することが可能になる。なお、図25（c）に示す統合利用条件は、チャネル送信契約情報に一致する。

【0206】これにより利用条件の修正の際にも効率的に最も良い利用条件を見つけることができる。例えば、「無期限の期間限定で1回コピー可で機器制限のない利用をしたい」という利用条件を、コピー制限、有効期限、機器制限の優先順位で統合する場合、まず1回コピー可の部分（真ん中6ビット）を参照し、そこが0でなければその中で有効期限を比較する。図25の例では、1回コピー可の条件は認められており、その中で有効期限が無制限のものを探すが、それは存在しない。そこで、許可されている有効期限の中で期間が最も長い1週間のものを選択する。1回コピー可で1週間の有効期限のものは機器限定ありとなしの2種類存在する。ここでは機器制限のない利用を希望しているので、機器制限なしを採用して、「1週間の期間限定で1回コピー可で機器制限のない」利用を統合されたコンテンツ利用条件として決定することができる。

【0207】このようにすれば、図13～図15のようなリストが不要になり、小さなメモリ領域しかない放送受信装置でも実現されるし、高速処理が可能となる。また、チャネル契約情報が格段に小さくなるため、送信が容易となる。なお、その分契約状態の種類は図13～図15のようなリストを用いる場合に比較して制限されるので、使われるシステムの要請によって両者を使い分けると効果的である。

【0208】また、システムによってはチャネル受信契約情報が含まれる受信契約関連情報パケットの送信帯域と、チャネル送信契約情報が含まれる番組関連情報パケットの送信帯域が異なっており、どちらか一方の通信路の送信量が少ない場合もある。このような場合には、送信量が少ない方の情報をビット形式で記述し、送信量が多い方を展開形式で記述する方式も考えられる。この場合、ビット形式の契約情報を一旦展開形式に直してマッチングする必要があるため、一般には異なる条件記述形式を統一形式に表現し直す処理を経る必要があり、条件統合の際にはその統一表現を使って前述と同様の手段で統合する。また、このような方式は、番組関連情報パケットとチャネル受信契約関連情報パケットの放送事業者が異なる場合などにも起こる。

【0209】＜バリエーション3＞次に、チャネル受信契約情報とチャネル送信契約情報の統合処理に関するバリエーションについて説明する。

【0210】前述した統合処理は、各項目に優先順位を付けて、優先度の高い利用条件を採用するものであった

27

が、各条件をアイテムとした評価関数を定義することによって、よりユーザの希望に近い利用条件を選択することができる。

【0211】以下では、評価関数を用いる方式を、ユーザ希望のコンテンツ利用条件が「1999年12月25日まで、5回まで、機器制限なし」とされた場合を例にとって説明する。

【0212】図26に、この場合の利用条件判定／修正部117における処理手順の一例を示す。なお、図26に示すアルゴリズムは、図12に示すアルゴリズムと置き換えるものであり、図11のアルゴリズムから処理が移される。

【0213】まず、入力されたチャネル受信契約情報とチャネル送信契約情報を統合して、図15に示すような利用可能契約情報リストを作成する（ステップS121）。

【0214】次に、作成された利用可能契約情報リストの各々の利用可能契約情報に対して評価値を計算する（ステップS122）。

【0215】まず、基本項目は「有効期限」「回数制限」「機器制限」の3つであり、それぞれ図27～図29に示すような基本評価値を与える（図29の3番目の評価値を0とする考え方もある）。

【0216】また、これらの基本評価値を、それぞれ $w_d$ 、 $w_t$ 、 $w_m$ という関数で置き換え、評価関数を $f(x) = 10w_d(x) + 5w_t(x) + 2w_m(x)$

のように定義すると、各利用可能契約条件の評価値が図30のように算出される。

【0217】本例の場合は、図30の評価値の中で最も高い値（150）を持つ「2000年1月7日までに、10回まで、機器限定で、視聴可能」（図30における下から2番目）という、利用可能契約情報が選択される（ステップS123）。本利用可能契約情報は、機器限定以外は、全て上記希望利用条件を満たしている。

【0218】ところで、次に高い評価値（140）を持つ利用可能契約情報は、「2000年1月7日までに3回まで機器限定なしで視聴可能」（図30における下から1番目）であり、回数制限のみが希望利用条件を満たしていない。これらの条件は評価値の差が10であり、このことから評価関数や基本評価値の取り方で出力される修正された利用条件の性質を変えることが理解できる。このことが評価関数を用いる利用条件の修正のメリットである。すなわち、利用者は評価関数を自分の好きなように適切に設定することにより、適切な利用条件の修正が自動的に行えるようになることを意味する。

【0219】なお、上記の例では希望利用条件で有限回数が指定されているが、希望利用条件で回数無制限が指定された場合には、図27に示す基本評価値をそのまま使うことができない。このような場合には、利用回数を

28

十分多い上限値、例えば100回、として計算する方法が考えられる。もちろん、この上限値が十分大きいかどうかは有効期限などの他の条件によって決まる。このため、有効期限などの他の条件を参照した上で、無制限の回数条件が指定された場合に基本評価値を参照する際の有限回数をフレキシブルに設定すると、より正確な利用条件の修正に貢献する。

【0220】また、より正確な利用条件を選択するという意味では、ユーザへの問い合わせ機能を持たせると好ましい。それを担うのはコンテンツ利用方法選択I/F106である。ここでは、コンテンツの希望利用条件を入力する他に、希望利用条件が満たされなかった際、評価値の高い順に利用条件を並び替え、図31のように表示することによりユーザにコンテンツ利用条件の自主的な選択を促す。

【0221】図32に、上記のような場合の処理手順の一例を示す。

【0222】まず、利用条件判定／修正部117は、チャネル受信契約情報とチャネル送信契約情報が入力されると、前述のような手段でそれらを統合し、利用可能契約情報リストを作成する（ステップS131）。

【0223】続いて、利用可能契約情報リストにある各々の利用可能契約情報に対して、前述した評価関数を用いて、評価値を算出する（ステップS132）。

【0224】ここで、算出した評価値が高い順に利用可能契約情報を並び替え（ステップS133）、並び替えられたリストをコンテンツ出力制御部118を経由してコンテンツ利用方法選択I/F106に送信する（ステップS134）。

【0225】コンテンツ利用方法選択I/F106では、画面に図31に例示するような利用方法選択画面を出力して、ユーザからの利用方法の選択を促す。ここで、評価値の高い順に表示されるので、ユーザは、次画面を表示しなくても、所望に近い利用形態を選択することができ、便利である。

【0226】なお、明らかに省略できる条件を特定してそれを省くことにより、より多くの選択子を出力することも可能である。図31の例の場合、第3・第4の利用条件がそれにあたり、すなわち、第4の条件が第3の条件の有効期限の制限になっており、選択条件としては無駄なものである（すなわち、第4の条件を省く）。これらは、条件を比較することにより決定可能であり、候補数が少なければ特定することは容易である。

【0227】＜バリエーション4＞次に、2次利用出力部121においてライセンス情報を作成する処理および構成のバリエーションについて説明する。

【0228】前述した実施形態では、ライセンス情報を、図17に例示するようにコンテンツに切り離されたデジタルデータとして扱っていた。しかし、これは出力の際にアナログ変換した後での利用制御には（ライセン

ス情報が切り離されてしまうので)利用できない。すなわち、前述の実施形態では、デジタル録画の制御はできるが、アナログ録画の制御は不可能である。そこで、アナログデータに変換されてもなお、2次利用制御ができる方式が重要となる。

【0229】一方で、主に画像や音声などのアナログデータにデータを埋め込む電子透かしという技術が近年注目を集めている(「電子透かしの基礎」(松井甲子雄著、森北出版、1998)等参照)。この技術を使うと、情報をアナログデータの中に目立たなく且つ容易に10は抜き取られないように、埋め込むことができる。すなわち、電子透かし技術を使うと、ライセンス情報をアナログデータの中に埋め込むことができるので、アナログデータになってもなお、利用管理ができるばかりか、物理的に分離されたライセンス情報を持たなくても良いので、管理も簡単である。

【0230】以下、電子透かしを使ったライセンス管理について説明する。

【0231】図33に、この場合の2次利用出力部121の構成例を示す。図33に示されるように、2次利用10出力部121は、コンテンツ入力部221、電子透かし埋め込み部222、コンテンツ暗号化部223、コンテンツ出力部224、機器マスター鍵格納部225、利用条件入力部226、利用条件生成部227を含む。

【0232】図34に、この場合の処理手順の一例を示す。

【0233】まず、利用条件入力部226からコンテンツ利用条件が入力されと(ステップS141)、利用条件生成部227に送られる。利用条件生成部227は、入力されたコンテンツ利用条件に機器限定があるかを判定30する(ステップS142)。ここで、機器限定の利用制限がある場合は、図20および図21の場合と同様に、機器IDを2次利用装置から取得し(ステップS143)、図18に例示したような形式で、ライセンス情報を生成する(ステップS144)。機器限定の利用制限がない場合は、そのままライセンス情報を生成する(ステップS144)。

【0234】次に、生成したライセンス情報を電子透かし生成部222に送り、コンテンツ入力部221から入力されたコンテンツに埋め込む(ステップS145)。40埋め込まれたコンテンツは、コンテンツ暗号化部223において、機器マスター鍵格納部209から取得した機器マスター鍵 $K_m$ で暗号化され(ステップS146、S147)、コンテンツ出力部224から出力される(ステップS148)。

【0235】以上のように構成することにより、処理も構成も簡単になる。なお、電子透かしでは画像の1枚毎に埋め込むので時間を要し、また、新たにライセンスを購入するなどしてコンテンツを再生利用する際には埋め50込んだ電子透かしを一旦外して、新たに作成した透かし

を埋め込む必要がある(これはライセンス情報がコンテンツ情報と分離していないために起こる)。このような状況においては、お互いの良い点を活かすため、ライセンスに含まれる限定項目の種類によってデジタルライセンスとして反映させるか、電子透かしでアナログレイヤに埋め込むかを決定して、運用するシステム構成も考えられる。

【0236】<バリエーション5>次に、2次利用装置側の機器信頼性に関して説明する。

【0237】本実施形態において、コンテンツ利用条件をライセンス情報という形で出力しても、2次利用装置においてそれが忠実に守られなくては意味がない。これは通常の機器接続においても言えることである。

【0238】近年検討されているデジタル機器間の接続に関する国際規格IEEE1394では、この点に鑑みて認証プロトコルを導入している。IEEE1394規格はデジタル機器間の入出力に関してプロテクション機構を設け、それらが転送されるバス上、接続ケーブル上においてもコピープロテクションすることを規格化している。

【0239】そこで、本実施形態において、放送受信装置と2次利用機器との間をIEEE1394バスで接続し、上記認証プロトコルを利用する方法も考えられる。

【0240】以下、バス、接続ケーブルのように機器間のデータ転送に利用される接続線を特に「接続回線」ということにする。

【0241】従来のDVDなどに記録される暗号化データは、DVD上から生データが直接読み込めないという意味では、コピープロテクションがなされているが、再生する際は、機器内で復号され、(デジタルTVなどの)外部機器に生のデータとして出力される。この場合、接続回線上で、当該生データを捕らえれば簡単にコピープロテクションが破られてしまう。このため接続回線上でもコンテンツを保護する立場から、接続機器間で互いに取り決めた暗号鍵によってコンテンツを暗号化して転送することにより、接続回線上でのコピープロテクションを実現しているのが、IEEE1394のコピープロテクション規格である。

【0242】しかし、いかに通信路上でコピープロテクションを行っても、出力する機器の設計の不備などの理由で暗号化したコンテンツが解読され、コンテンツが生50の状態である状態にあれば意味がない。したがって、相手の機器の機種が別途得られた無効機器リスト

(リボケーションリスト)に含まれているか否かを判断し、含まれている場合には、出力を拒絶する。含まれていない場合には、接続されている機器が本当にその機種であるかを確かめるために、チャレンジデータを相手の機器に出力し、当該機種しか知り得ない情報を使って、当該チャレンジデータにデジタル署名を付けてもらい、それを送り返してもらい、その署名を検証することによ

り、認証を行う。

【0243】ただし、ここで1つの機器が全ての機種の公開鍵を保持しておくことは現実的ではないので、実際上は接続機器から公開鍵を取得する。ただし、公開鍵は署名の検証鍵でもある一方で、公開鍵と秘密鍵のペアは比較的簡単に生成できる事実があるので、別の機種のマシンが当該機種を偽って公開鍵を送信するというプロテクト破りの手法が考えられる。このため、それぞれの機種は、発売時に、公開鍵と秘密鍵のペアを作成し、IEEE1394が定める管理機関に公開鍵を示して、デジタル証明書を発行してもらい、それを送信するという認証方法を採用している。デジタル証明書には管理機関の持つ秘密鍵でデジタル署名が施されており、対応する公開鍵が全ての機器に予め含まれているので、当該公開鍵が含まれるデジタル証明書を認証することにより、当該公開鍵が正しいものかどうかを判断することができる。

【0244】また、デジタル署名の作成には、大きく分けて、公開鍵暗号を使う方式と、共通鍵暗号を使う方式があり、前者は後者よりも処理時間がかかるが、安全がより高いため、計算能力の高い（主に据え置き型の）機種、後者は安全性は劣るが、処理能力が低い機種でも実行できるので、計算能力の低い（主に携帯型の）機種に適用される。認証の後には互いに共通に知る情報（例えば公開鍵）を基に鍵の交換プロトコルを実行し鍵を交換し、その鍵を使ってコンテンツを暗号化して転送する。

【0245】IEEE1394を利用する場合、本実施形態における機器間の転送もIEEE1394に準拠しなくてはならない。この意味で共通化でき、本実施形態でも必要となるのは機器認証の部分である。すなわち、前述したように、本実施形態において2次利用の制限を行っても、2次利用装置がそれを実行しない、もしくは簡単な改造によって実行されないようにできてしまう場合には、当該機種の機器には2次利用させるべきではない。ただし、この場合であっても、コピープロテクションは正常に動作する可能性もあるので、無効機器リストをIEEE1394とは別に配布することが望ましい。そのためには、専用にバケットを定義し、放送によって送信すれば効果的である。また、上記でコンテンツの暗号化鍵として定めたコンテンツ鍵 $K_c$ をIEEE1394プロトコルで生成される共有鍵とすることもできる。その場合は、本実施形態の2次利用出力部121が作成するコンテンツ鍵 $K_c$ で暗号化した上にIEEE1394が定める転送鍵でさらに暗号化する必要がなくなり、処理を省くことができる。

【0246】以下では、上記の認証プロセスを導入した場合のコンテンツ出力制御部118について説明する。

【0247】図35に、この場合のコンテンツ出力制御部118の構成例を示す。図35に示されるように、コンテンツ出力制御部118は、利用条件入力部301、出力判定部302、機器認証部303、利用情報出力部

304を含む。

【0248】図36に、この場合の処理手順の一例を示す。

【0249】コンテンツ出力制御部118の利用条件入力部301からコンテンツ利用条件が入力され（ステップS151）、出力判定部302においてコンテンツの出力判定が行なわれる。実際の出力判定は、利用条件判定／修正部117により行なわれる。

【0250】ここで、利用可能でなく（ステップS152）、かつ修正不可能ならば（ステップS153）、利用不許可の出力を2次利用出力部121に行ない（ステップS154）、処理を終了する。

【0251】それ以外の場合は、希望通りかもしくは修正された利用条件が得られ（ステップS152、S153、S155）、出力判定部302において、後述する機器認証部303の機器認証の結果に基づいてコンテンツを出力して良いか否かの判定を行ない（ステップS156）、出力可となれば、コンテンツ利用条件を利用条件出力部304から2次利用出力部121へ出力する（ステップS157）。出力不許可の場合は、利用不許可の旨を示す信号を2次利用出力部121へ出力する（ステップS154）。

【0252】一方、機器認証部303は、コンテンツ利用条件が入力された時点から上記のプロセスとは独立に、放送受信装置から2次利用装置の認証を行なう（ステップS158）。

【0253】認証は、まず、2次利用装置から機種IDを出力してもらい、当該機種IDの2次利用装置が安全な装置か否かの判定を受信装置内部に持つ安全でないIDの一覧を示したリボケーションリストを参照して行なわれる。ここで、安全な機種であるとされた場合は、接続されている機種が確かに当該IDを持つ機種であることを確認する。この確認には、デジタル署名技術が用いられる。

【0254】デジタル署名技術については、例えば次のような実現形態が考えられる。まず、放送受信装置はランダムに選んだメッセージを2次利用装置に送り、当該IDを持った2次利用装置しか知り得ない秘密情報を使って暗号化して返送してもらう。そして、返送された暗号文を放送受信装置が持つ対応した鍵を使って復号して検証することによって、確かに当該IDを持つ2次利用装置が接続されていることを認証することができる。

【0255】ここで、認証されなければ（ステップS159）、2次利用装置が不認証であった旨の信号を2次利用出力部に出力して終了する（ステップS161）。認証された場合は、同様の処理を2次利用装置側から行ない（ステップS160）、放送受信装置は2次利用装置側から送られて来たランダムメッセージを受信装置が持つ認証用の秘密鍵で暗号化して送信する。このことにより、2次利用装置側から受信装置が認証されれば（ス



テップS163)、利用条件の出力を許可しても良い旨の信号を出力判定部302に送る。そうでない場合は、放送受信装置が不認証であった旨の信号を2次利用出力部121に送り(ステップS162)、処理を終了する。

【0256】さらに、認証の際、受信装置から2次利用装置を認証するだけの構成も考えられる。一般には、認証は処理時間のかかる処理であるので、片方向だけであると処理が半分となる。また、放送受信装置は放送局から送信されてきたデータを秘密データを使って復号でき10 10 という意味からは、既に放送局によって認証されているものと考えることができるからである。

【0257】＜バリエーション6＞これまでの説明では、チャンネル送信契約情報は、対応するコンテンツと同時性を持って放送されるものとしたが、チャンネル送信契約情報を例えばEPG(Electronic Program Guide:電子番組ガイド)に含めて予め放送するようにしてもよい。

【0258】以下では、予めチャンネル送信契約情報を放送し、コンテンツの放送に先だって、コンテンツ利用条件を決定可能とした実施形態について、録画予約の際にコンテンツ利用条件を決定する場合を例にとりて説明する。20

【0259】図37に、録画予約機能を持つ放送受信装置の構成例を示す。本放送受信装置は、基本的には、図1の構成と同様であるので、相違する点についてのみ説明する。

【0260】図38に、チャンネル送信契約情報を含む電子番組ガイド情報の構造例を示す。

【0261】電子番組ガイド情報パケットは、図7に示すように、情報識別子、チャンネル識別子、コンテンツ識別子、チャンネル送信契約情報、番組情報からなっている。情報識別子、チャンネル識別子、コンテンツ識別子、チャンネル送信契約情報は、これまでと同様である。番組情報は、対応するコンテンツに関する情報で、例えば、タイトル、放送開始日時、放送終了日時、ジャンル、出演者といったような情報である。電子番組ガイド情報は、例えば、契約チャンネルで放送される。また、電子番組ガイド情報パケットは、暗号化しないものとする。

【0262】なお、チャンネル送信契約情報は、番組関連情報パケットにも含めてもよいし、電子番組ガイド情報パケットでのみ放送するようにしてもよい。

【0263】また、ここでは、コンテンツパケットと、その他のチャンネル送信契約情報を含むパケット(コンテンツ対応の情報を含むパケット)には、コンテンツ識別子を付加するものとする。

【0264】さて、図37においては、電子番組ガイド情報パケットを受信した場合、フィルター部111から番組関連情報復号部113を経由して、番組情報および各識別子がコンテンツ利用法選択I/F106へ渡さ20

れ、コンテンツ利用法選択I/F106において蓄積される。また、チャンネル送信契約情報および各識別子が送信契約情報格納部128に蓄積される。

【0265】そして、例えば、ユーザが録画予約を行う場合、番組指定や録画先などの通常の操作の他に、希望するコンテンツ利用条件の入力を行う。以降は、既に説明した処理と同様にコンテンツ利用条件の判定や修正などが行われ、最終的に当該コンテンツに対するコンテンツ利用条件が決定される。

【0266】なお、この時点あるいはそれ以降の適当なタイミングで、ライセンス情報を作成する。

【0267】次に、コンテンツ利用法選択I/F106、録画予約されたコンテンツの放送開始時刻を監視し、あるいは該コンテンツの識別子が受信されたかどうかを監視し、放送開始時刻(もしくはその一定時間前)になった場合、あるいは該コンテンツの識別子が受信された場合に、録画を開始する。すなわち、コンテンツを暗号化し、暗号化コンテンツとライセンス情報を、録画機器に送信する。

【0268】以降は、録画機器において、与えられたライセンス情報に従って、コンテンツの利用が行われる。

【0269】＜バリエーション7＞次に、チャンネル受信契約情報の圧縮手法に関して説明する。

【0270】これまででは、チャンネルとチャンネル受信契約情報が1対1に対応する場合を想定して説明したが、この場合には、サイズの比較的大きくなる可能性のあるチャンネル受信契約情報を1チャンネル毎に対応して配送することから、契約者数、チャンネル数、チャンネル受信契約情報の大きさ、配信頻度などと、通信路の送信帯域との関係によっては、チャンネル受信契約情報の送信量が通信路の送信帯域を圧迫することもある。

【0271】そこで、以下では、複数のチャンネルに共通のチャンネル契約情報を送信する方法について説明する。

【0272】ところで、例えばチャンネル数の多いCS放送では、数種類のパッケージ(複数のチャンネルのセット)を設け、そのパッケージを単位として契約することがほとんどである。

【0273】ここでは、このようなシステムに適応することを想定し、図3のチャンネル識別子の代わりに、パッケージ識別子を導入する場合を例にとりて説明する。

【0274】パッケージとは、複数のチャンネルのセットのことであり、パッケージ識別子はパッケージを識別するための識別子である。

【0275】さらに、当該パッケージ識別子のパッケージにどのチャンネルが含まれるかを記述したパッケージ定義情報は別途送信されるものとする。ただし、ここでは説明を簡明にするために、図2に示すようなビット列をパッケージ識別子とする。この場合、ビット列で1が立っているビット位置に対応したチャンネル(図2では、2チャンネル、5チャンネル、7チャンネル、8チャンネル)が当20



35

該パッケージに含まれているチャンネルを意味するものとする。

【0276】このようにすることで、複数のチャンネルのチャンネル受信契約情報をまとめて送信することができるため、送信量削減の観点から有効である。もちろん、このようなシステムにおいても、チャンネル毎に個別のチャンネル受信契約情報を送信することは可能で、なぜなら、8ビットのうち当該チャンネルに対応したビットだけを1にすればよい。

【0277】パッケージ識別子を導入するため変更する処理は、図1における受信契約関連情報復号部において、チャンネル識別子とチャンネル受信契約情報をセットにして受信契約情報格納部に格納していた部分を、パッケージ識別子を解釈して、チャンネル毎の記述形式に直し、受信契約情報格納部に格納するように変更すればよい。

【0278】また、パッケージ識別子を導入した場合、ワーク鍵との対応が問題になる。この場合、同じパッケージに含まれるチャンネルは同じワーク鍵とする方法と、前記のようにワーク鍵がチャンネル毎に異なることを前提とし、契約に応じて個別契約者に対応するチャンネルのワーク鍵を契約者の放送受信装置が持つマスター鍵で暗号化して別途送信する方式が考えられる。

【0279】(第2の実施形態) 本実施形態の放送受信装置の2次利用に関する処理および各情報に対する処理等は、基本的には第1の実施形態と同様であるので、以下では相違する点もしくは追加する点を中心に説明する。

【0280】第1の実施形態では、各放送受信装置が個別のマスター鍵を有する方式を想定したが、本実施形態では、全ての受信装置が共通のマスター鍵を有する方式を想定して説明する。このような限定受信システムにおいては、各受信装置対し、個別に契約情報を暗号化して送信する必要がないので、限定受信の送信量が少なくてすむという利点がある。また、本実施形態では、デジタル署名などの偽造防止技術を用いて、そのマスター鍵が破られた際の安全性への対策を行っている。

【0281】第1の実施形態では、図5のような3段の鍵構成を採用したが、本実施形態では、このような限定受信のために、図39のような2段の鍵構成を採用する。すなわち、チャンネルキー $K_{ch}$ とチャンネル受信契約情報を全ての受信装置に共通のマスター鍵 $K_M$ で暗号化して送信する。送信されたチャンネルキーを使って放送コンテンツを復号する。

【0282】以下、この限定受信システム上で第1の実施形態と同様にチャンネル受信契約情報とチャンネル送信契約情報とを統合することに限定受信として2次利用に対する制御を実現する例を示す。

【0283】第1の実施形態では、放送受信装置は、コンテンツパケット(図6)、番組関連情報パケット(図7)、受信契約関連情報パケット(図8)を受信した

36

が、本実施形態においては、これらに対応するものとして、放送受信装置は、図40に示すようなコンテンツパケットと図41に示すような受信契約関連情報パケットを受信する。

【0284】コンテンツパケットは、図40に示されるように、情報識別子、チャンネル識別子、チャンネルキー識別子、チャンネル送信契約情報 $C_s$ 、放送コンテンツからなっており、チャンネル送信契約情報から放送コンテンツまでの部分をチャンネルキー $K_{ch}$ で暗号化している。なお、各情報の意味と役割は第1の実施形態と同じであるので、ここではその説明は省略する。

【0285】第1の実施形態と相違し、本実施形態においては、チャンネル送信契約情報がコンテンツパケットに含まれる。これは鍵構造が2段であることによる必然性もあるが、コンテンツと当該コンテンツのチャンネル送信契約情報とが物理的にリンクしているので、システムとしても構成しやすいという利点もある。

【0286】受信契約関連情報パケットは、図41に示されているように、情報識別子、マスター鍵識別子、チャンネル識別子、チャンネルキー識別子、チャンネルキー、契約情報の数 $n$ 、 $n$ 個の契約情報、デジタル署名からなっており、チャンネル識別子からデジタル署名までの部分をマスター鍵で暗号化している。

【0287】デジタル署名は、契約情報数 $n$ および契約情報1～契約情報 $n$ までの部分に関してのデジタル署名である。デジタル署名は、契約情報の偽造を防ぐためのものであり、契約情報を1ビットでも変更するとデジタル署名が検証できなくなるという性質を持っている。さらに、デジタル署名を作成するには放送局側にしか存在しない秘密鍵を知らなくてはできないため、デジタル署名を付加することにより契約情報の偽造を防ぐことができる。

【0288】ここで、「契約情報」とは、図42に示されるように、受信装置IDとチャンネル受信契約情報からなっており、受信装置IDに対応するチャンネル受信契約情報を表している。

【0289】なお、受信契約関連情報に含まれるその他の各情報の意味と役割は第1の実施形態と同じであるので、ここではその説明は省略する。

【0290】図43に、本実施形態に係る放送受信装置の構成例を示す。

【0291】図43に示されるように、本放送受信装置は、受信部101、A/D変換部102、誤り検出/訂正部103、チャンネル選択部104、チャンネル選択インタフェース(I/F)105、限定受信処理部(限定受信チップ)106、コンテンツ利用法選択インタフェース(I/F)107、コンテンツ利用条件表示部108を有する。また、限定受信処理部100すなわち限定受信チップには、フィルター部111、デスクランブル部112、受信契約関連情報認証部114、受信契約関連

情報復号部115、受信契約判定部116、利用条件判定/修正部117、コンテンツ出力制御部118、チャンネル情報入力部119、標準出力部120、2次利用出力部121、マスター鍵格納部122、受信装置ID格納部123、チャンネルキー格納部125、チャンネルキー出力部126、受信契約情報格納部127、送信契約情報格納部128、送信契約情報抽出部129が作り込まれ、耐タンパー性が付与されている。

【0292】以下、本実施形態の放送受信装置の動作について説明する。

【0293】図44～図46に、本実施形態の放送受信装置の動作手順の一例を示す。

【0294】本実施形態の放送受信装置は、放送波を受信後(ステップS201)、A/D変換を行なってデジタルデータに変換して(ステップS202)、誤り検出および誤り訂正を行なって(ステップS203)、フィルタ部111においてパケット内の情報識別子によってコンテンツパケットであれば(ステップS204)、チャンネル識別子を参照して、視聴チャンネルのコンテンツかどうかを判定し(ステップS205)、視聴チャンネルであった場合はデスクランブル部112へ送信する(ステップS206)。そうでない場合は、当該パケットに関する処理を終了する。受信契約関連情報パケットであった場合は(ステップS207)、契約関連情報に送信する(ステップS208)。

【0295】次に、視聴チャンネルのコンテンツパケットの処理に関して図45のフローチャートに従って詳しく説明する。

【0296】コンテンツパケットがデスクランブル部112に入力されると、デスクランブル部112ではチャンネルキー出力部126へチャンネルキーの出力の要請を行なう(ステップS211)。チャンネルキー出力部126では、受信契約判定部116に対してチャンネル識別子を入力し、受信契約情報格納部127から当該チャンネルのチャンネル受信契約情報を取得して、契約フラグが1である場合、チャンネルキーの出力許可信号を出し、0である場合はチャンネルキーの出力不許可信号を出す(ステップS212～S217)。チャンネルキー出力不許可信号が入力された場合、チャンネルキー出力部126では当該パケットに関する処理を終了する。

【0297】チャンネルキーの出力許可信号がチャンネルキー出力部126へ入力された場合は、チャンネルキー出力部126はチャンネルキー格納部125へチャンネル識別子とチャンネルキー識別子を送り、チャンネルキーを取得しデスクランブル部112へ送り(ステップS218)、デスクランブル部112においてコンテンツのデスクランブルを行なう(ステップS219)。

【0298】送信契約情報抽出部129は、デスクランブルされたコンテンツにチャンネル送信契約情報が含まれているか否かを情報識別子で判定し(ステップS22

0)、含まれている場合チャンネル送信契約情報を取得し、送信契約情報格納部128へ格納する(ステップS221)。

【0299】次に、コンテンツはコンテンツ出力制御部118へ送られ、第1の実施形態と同様の方法で、当該コンテンツについてコンテンツ利用情報をチェックする(ステップS222)。チェックした結果、利用不許可であれば、コンテンツ利用条件表示部107に利用不許可の表示を行ない、処理を終了する。許可された場合は、利用形態とコンテンツとともに標準出力であるか2次利用出力であるかによって(ステップS223)、それぞれ、標準出力部120、2次利用出力部121に出力される。

【0300】2次利用出力部121に出力された場合は、第1の実施形態と同様の処理でライセンス情報とそれに対応したコンテンツを生成し(ステップS224)、2次利用装置に出力して(ステップS225)、処理を終了する。

【0301】次に、受信契約関連情報パケットの処理に関して図46のフローチャートに従って詳しく説明する。

【0302】受信契約関連情報が受信契約関連情報復号部114に入力されると受信契約関連情報復号部114ではマスター鍵識別子をキーにして、マスター鍵格納部122からマスター鍵 $K_M$ を取得して(ステップS231)、暗号化部分を復号する(ステップS232)。復号された受信契約関連情報からチャンネルキー、チャンネル識別子、チャンネルキー識別子を抽出し(ステップS233)、チャンネルキー格納部125に格納する(ステップS234)。

【0303】次に、契約情報数 $n$ からデジタル署名までの部分を受信契約情報認証部115へ送付する。

【0304】受信契約情報認証部115では契約情報数 $n$ を抽出し、それを変数MAXに代入する。引続き契約情報を次々参照し、それらに含まれる受信装置IDと受信装置ID格納部123にある受信装置IDを比較して(ステップS236～S239)、一致した場合、デジタル署名を検証後(ステップS240、S241)、対応するチャンネル受信契約情報 $C_R$ を受信契約情報格納部127へ格納する(ステップS242)。自受信装置の受信装置IDと一致する契約情報がない場合や、デジタル署名が検証できなかった場合は、その時点で処理を終える。

【0305】なお、第1の実施形態において示したバリエーションは、本実施形態にも適用可能である。

【0306】なお、本実施形態において、チップ化しなくてよい処理機能の部分(例えば、ユーザインタフェースに関する部分など)は、ソフトウェアを利用しても実現可能である。また、そのような処理機能の部分は、コンピュータに所定の手段を実行させるための(あるいは

コンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための) プログラムを記録したコンピュータ読取り可能な記録媒体としても実施することもできる。

【0307】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0308】

【発明の効果】本発明によれば、あるチャネルに対して契約者が持っている1または複数の第1の利用条件と、あるコンテンツに対して規定されている1または複数の第2の利用条件とを統合することによって、契約者とコンテンツのペア毎に様々な限定受信を実現することができる。このことにより、コンテンツの価値などに応じてコンテンツ毎に利用制御することが可能になり、また、従来は十分にできていなかったコンテンツの2次利用などへも限定受信を拡張することができる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係る放送受信装置の構成例を示す図

【図2】チャネル展開情報の一例を示す図

【図3】チャネル契約情報のデータ構造例を示す図

【図4】コンテンツ利用情報のデータ構造例を示す図

【図5】放送コンテンツの暗号化機構について説明するための図

【図6】放送コンテンツパケットのデータ構造例を示す図

【図7】番組関連情報パケットのデータ構造例を示す図

【図8】受信契約関連情報パケットのデータ構造例を示す図

【図9】同実施形態に係る放送受信装置における放送受信からパケットの内容に応じた処理までの全体的な処理手順の一例を示すフローチャート

【図10】放送コンテンツパケットに対する処理手順の一例を示すフローチャート

【図11】利用条件判定／修正部における処理手順の一例を示すフローチャート

【図12】利用条件判定／修正部における処理手順の一例を示すフローチャート

【図13】チャネル受信契約情報におけるコンテンツ利用条件一例を示す図

【図14】チャネル送信契約情報におけるコンテンツ利用条件の一例を示す図

【図15】利用可能契約情報リストの一例を示す図

【図16】抽出結果リストの一例を示す図

【図17】ライセンス情報のデータ構造例を示す図

【図18】コンテンツ利用条件の一例を示す図

【図19】放送受信装置から2次利用装置へ渡される暗号化コンテンツのデータ構造例を示す図

【図20】2次利用出力部の内部構成の一例を示す図

【図21】ライセンス情報を作成する処理手順の一例を示すフローチャート

【図22】コンテンツを暗号化する処理手順の一例を示すフローチャート

【図23】番組関連情報パケットに対する処理手順の一例を示すフローチャート

【図24】受信契約関連情報に対する処理手順の一例を示すフローチャート

【図25】コンテンツ利用条件の他の表現形式を示す図

【図26】利用条件判定／修正部における処理手順の他の例を示すフローチャート

【図27】有効期限に対する基本評価値の一例を示す図

【図28】回数制限に対する基本評価値の一例を示す図

【図29】機器限定に対する基本評価値の一例を示す図

【図30】利用可能契約情報リストの他の例を示す図

【図31】利用可能契約情報選択画面の一例を示す図

【図32】利用条件判定／修正部における処理手順のさらに他の例を示すフローチャート

【図33】2次利用出力部の内部構成の他の例を示す図

【図34】2次利用出力部における処理手順の一例を示すフローチャート

【図35】コンテンツ出力制御部の内部構成の一例を示す図

【図36】コンテンツ出力制御部における処理手順の一例を示すフローチャート

【図37】同実施形態に係る放送受信装置の他の構成例を示す図

【図38】チャネル送信契約情報を含む電子番組ガイド情報の構造例を示す図

【図39】放送コンテンツの暗号化機構について説明するための図

【図40】放送コンテンツパケットの他のデータ構造を示す図

【図41】受信契約関連情報パケットの他のデータ構造例を示す図

【図42】契約情報のデータ構造例を示す図

【図43】同実施形態に係る放送受信装置のさらに他の構成例を示す図

【図44】同実施形態に係る放送受信装置における放送受信からパケットの内容に応じた処理までの全体的な処理手順の一例を示すフローチャート

【図45】放送コンテンツパケットに対する処理手順の一例を示すフローチャート

【図46】受信契約関連情報に対する処理手順の一例を示すフローチャート

【符号の説明】

101…受信部

102…A/D変換部

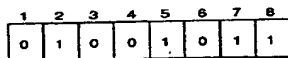
103…誤り検出／訂正部

104…チャネル選択部

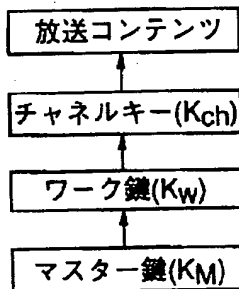
41

105...チャンネル選択インタフェース  
 106...限定受信処理部(限定受信チップ)  
 107...コンテンツ利用法選択インタフェース  
 108...コンテンツ利用条件表示部  
 111...フィルタ部  
 112...デスクランブル部  
 113...番組関連情報復号部  
 114...受信契約関連情報認証部  
 115...受信契約関連情報復号部  
 116...受信契約判定部  
 117...利用条件判定/修正部  
 118...コンテンツ出力制御部  
 119...チャンネル情報入力部  
 120...標準出力部  
 121...2次利用出力部  
 122...マスター鍵格納部  
 123...受信装置ID格納部  
 124...ワーク鍵格納部  
 125...チャンネルキー格納部

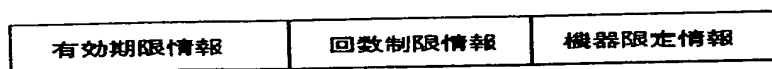
【図2】



【図5】



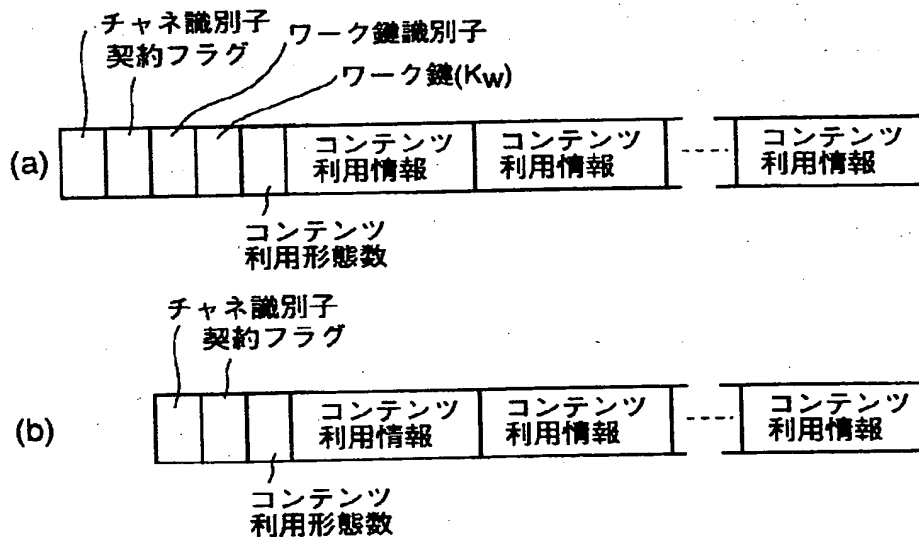
【図4】



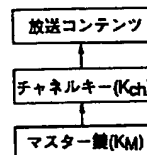
42

\* 126...チャンネルキー出力部  
 127...受信契約情報格納部  
 128...送信契約情報格納部  
 129...送信契約情報抽出部  
 201, 221...コンテンツ入力部  
 202, 223...コンテンツ暗号化部  
 203, 224...コンテンツ出力部  
 204...コンテンツキー生成部  
 205, 226, 301...利用条件入力部  
 206, 227...利用条件生成部  
 207...コンテンツID生成部  
 208...ライセンス情報生成部  
 209, 225...機器マスター鍵格納部  
 210...ライセンス情報出力部  
 222...電子透かし埋め込み部  
 302...出力判定部  
 303...機器認証部  
 304...利用情報出力部

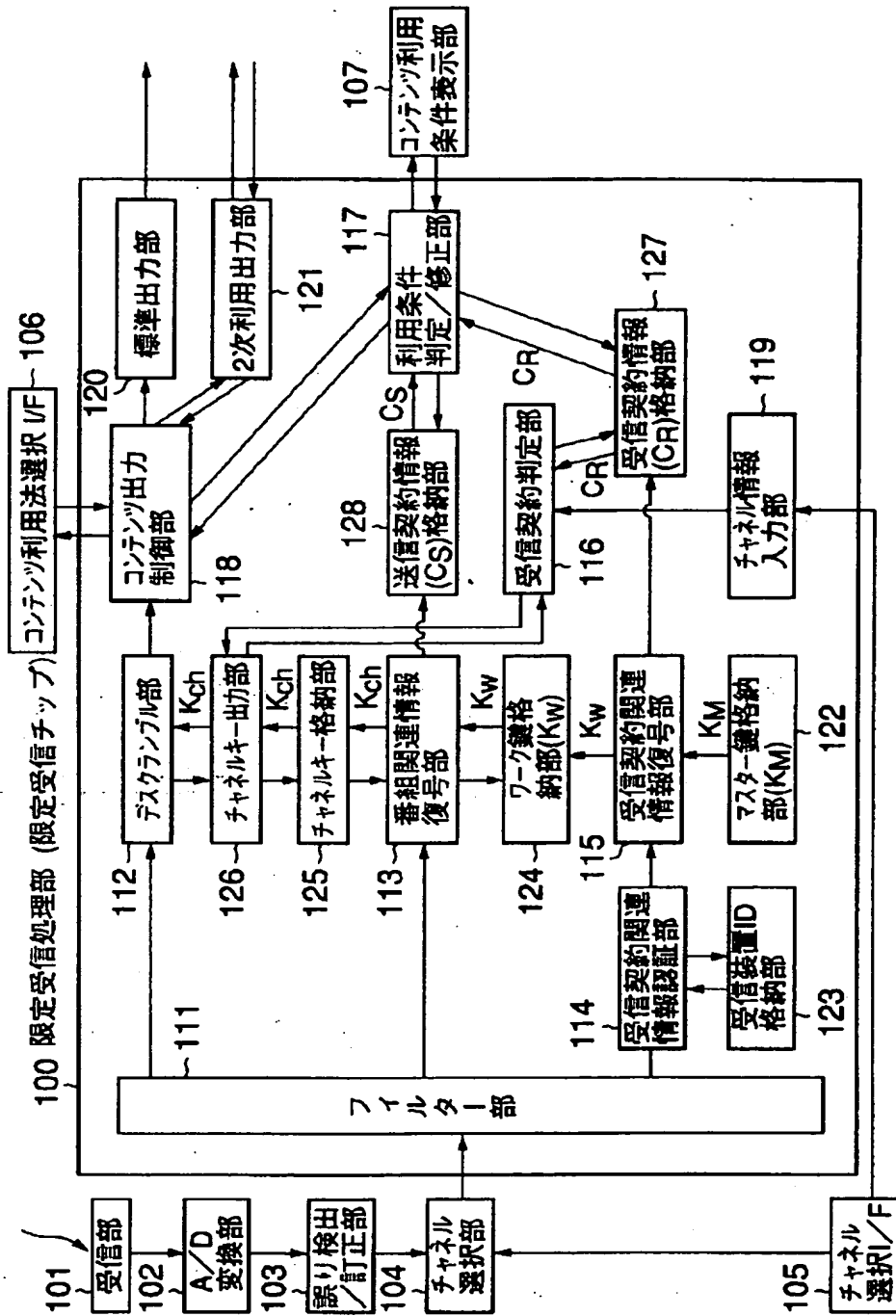
【図3】



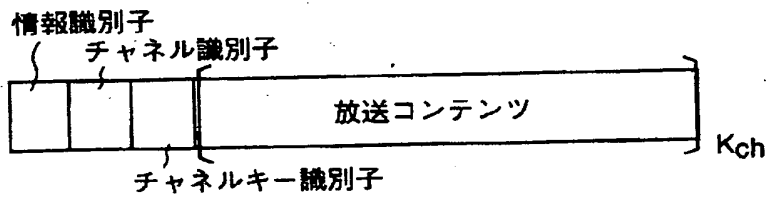
【図3 9】



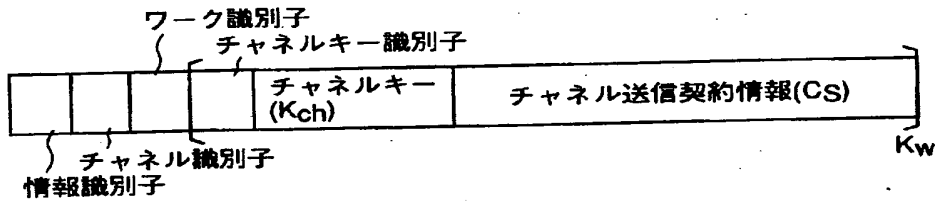
【図1】



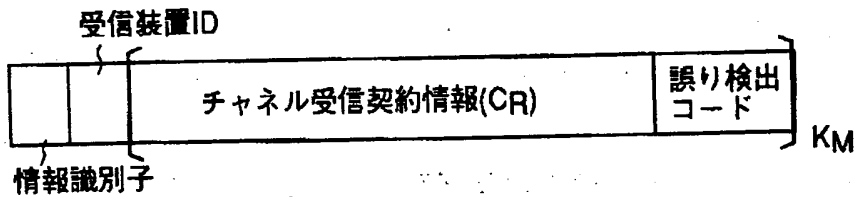
【図 6】



【図 7】



【図 8】



【図 13】

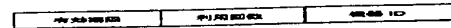
チャンネル受信契約情報

有効期限情報	回数制限情報	機器限定情報
1999.06.10	-1	0
-1	3	1
2000.01.07	10	0

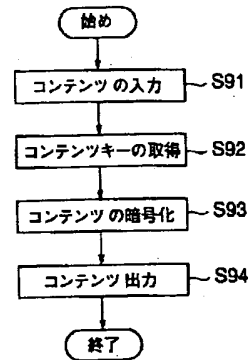
【図 16】

有効期限情報	回数制限情報	機器限定情報
1999.05.20	-1	0
1999.08.10	-1	1

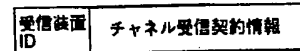
【図 18】



【図 22】



【図 42】

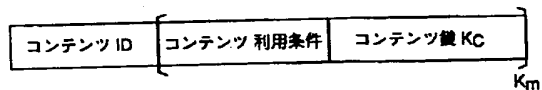


【図 14】

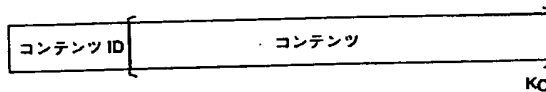
チャンネル送信契約情報

有効期限情報	回数制限情報	機器限定情報
1999.05.20	-1	0
1999.07.31	-1	1
2000.01.07	15	1
-1	3	0

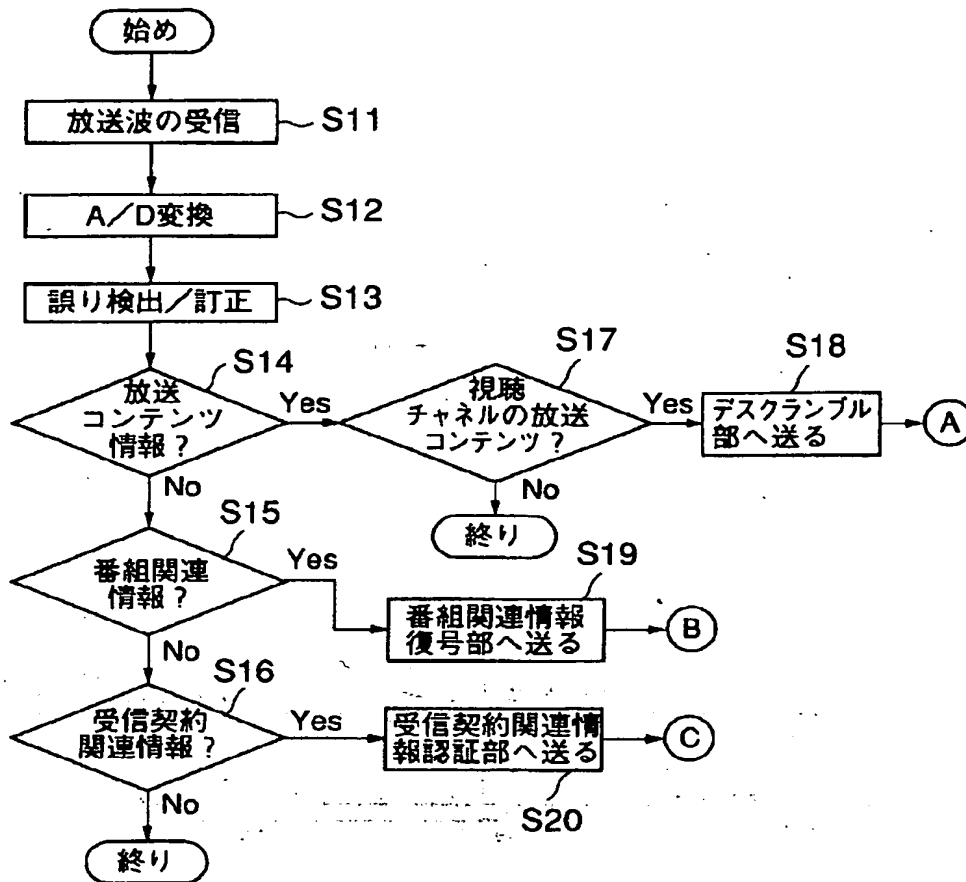
【図 17】



【図 19】



【図9】

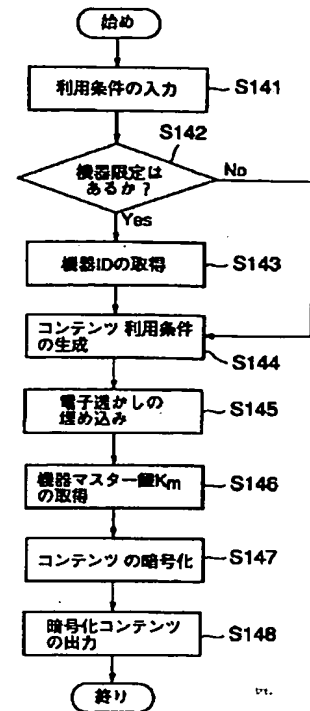


【図15】

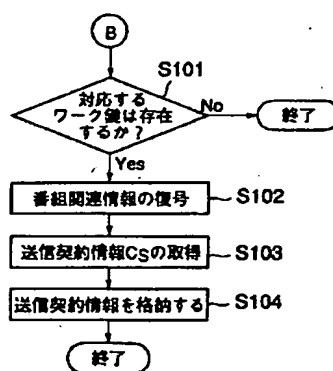
利用可能契約情報リスト

有効期限情報	回数制限情報	機器限定情報
1999.05.20	-1	0
1999.06.10	-1	1
1999.06.10	15	1
1999.06.10	3	0
1999.05.20	3	1
1999.07.31	3	1
2000.01.07	3	1
-1	3	1
1999.05.20	10	0
1999.07.31	10	1
2000.01.07	10	1
2000.01.07	3	0

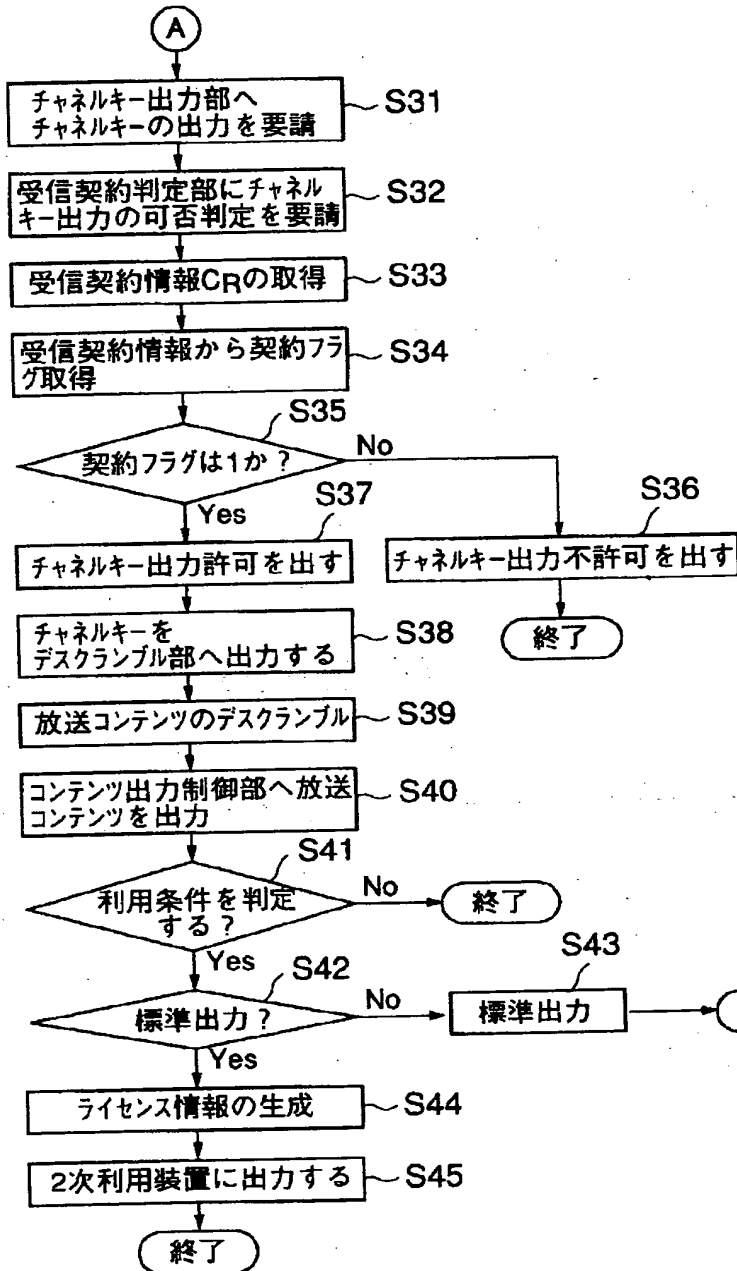
【図34】



【図23】



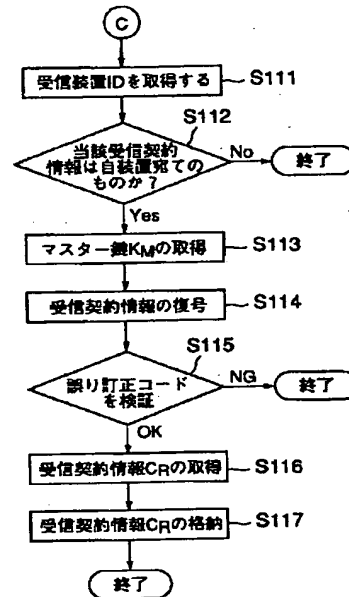
【図10】



【図38】

情報識別子	チャンネル識別子	コンテンツ識別子	チャンネル送信契約情報(CS)	番組情報
-------	----------	----------	-----------------	------

【図24】



【図27】

有効期限の基本評価値

有効期限との差	評価値
なし	10
3日以内	7
10日以内	3
それ以外	0

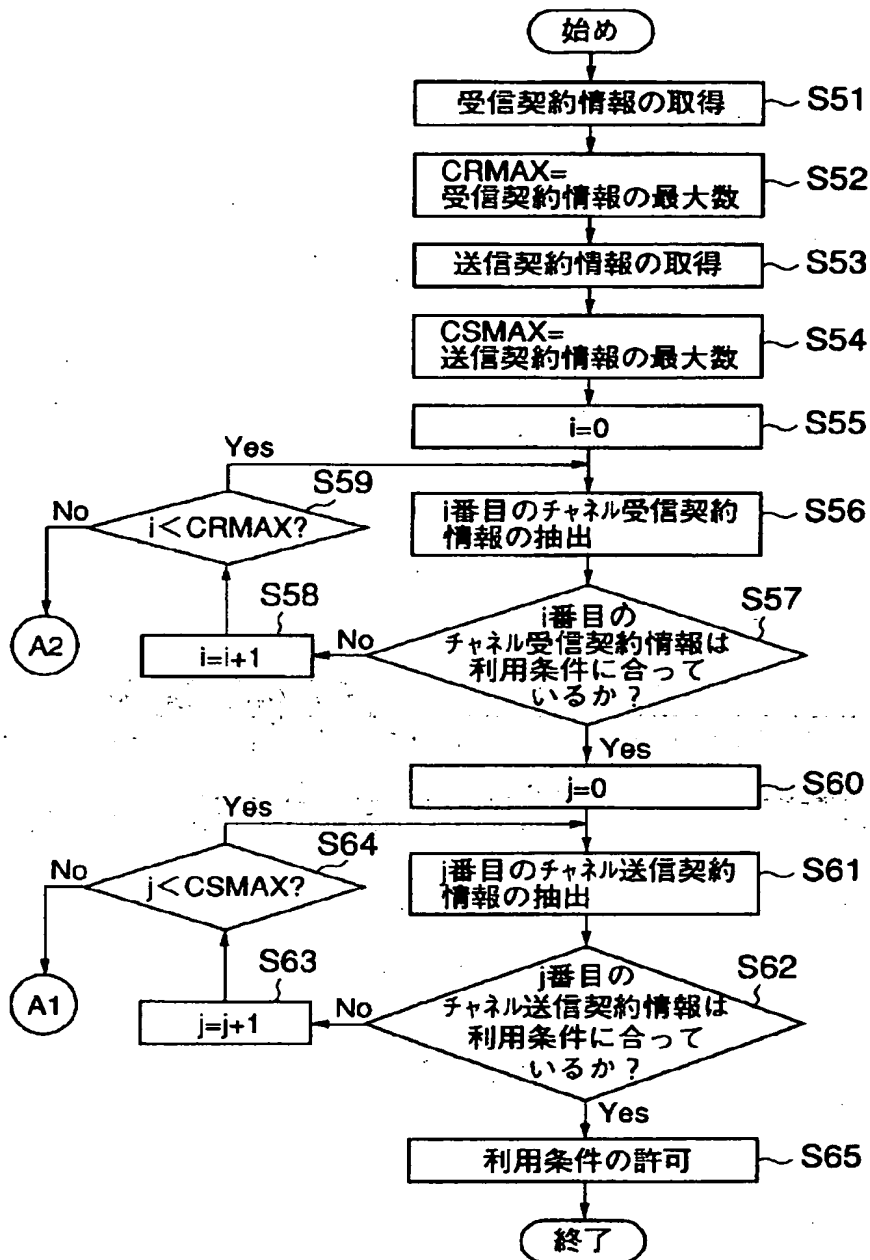
【図28】

回数制限の基本評価値

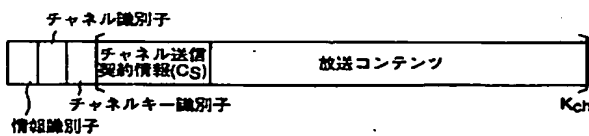
回数制限との差	評価値
なし	10
3回以内	4
10回以内	1
11回以上	0



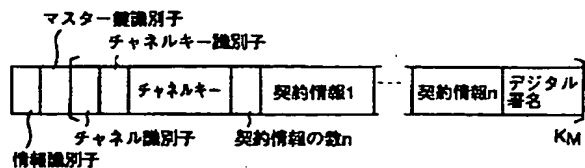
【図11】



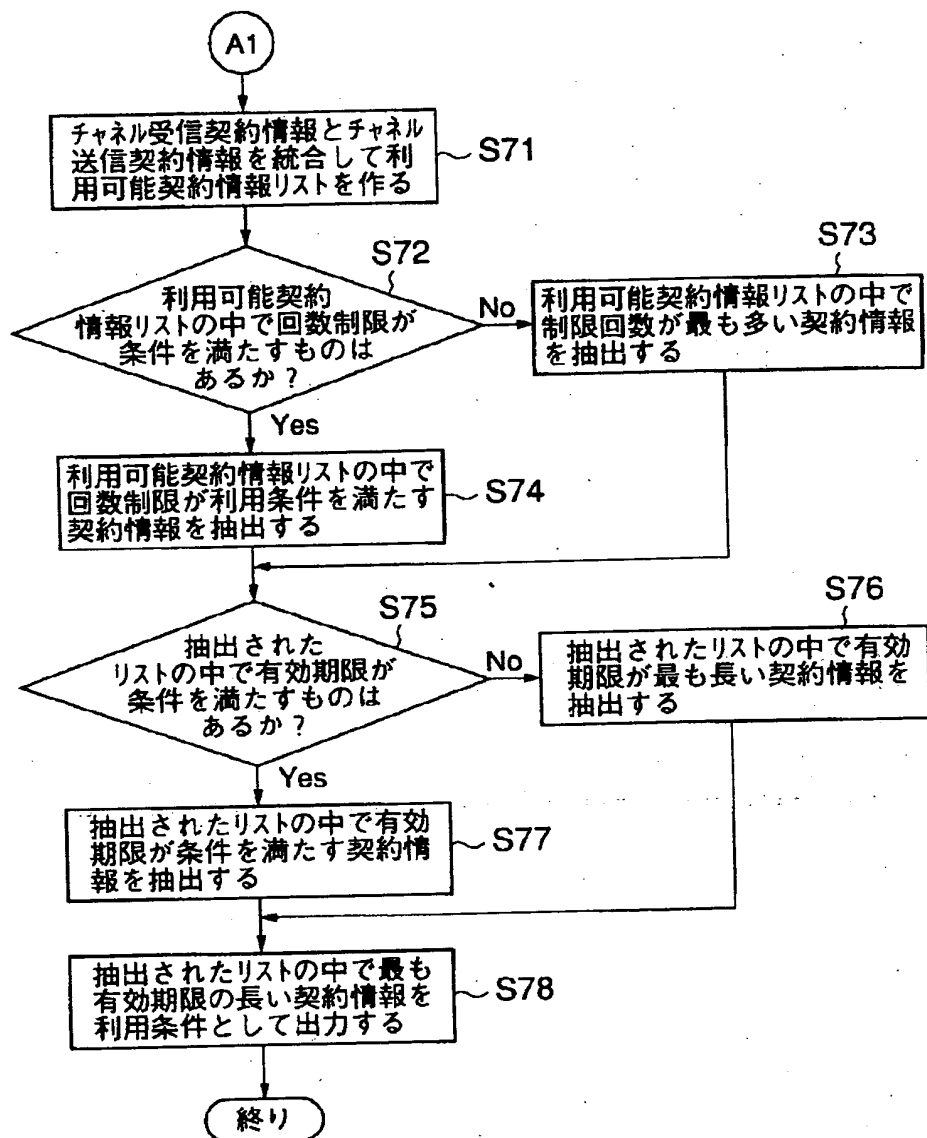
【図40】



【図41】



【図12】

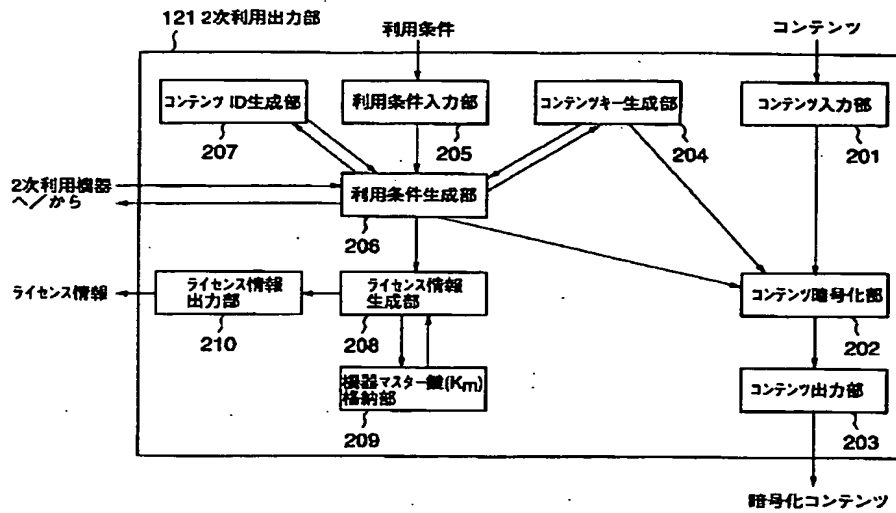


【図29】

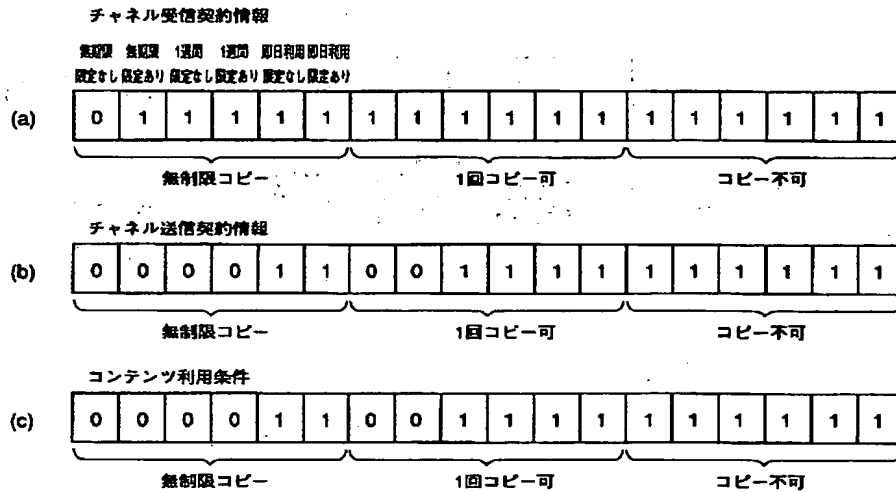
機器限定の基本評価値

利用条件の機器限定	希望条件の機器限定	評価値
1	1	10
1	0	0
0	1	10
0	0	10

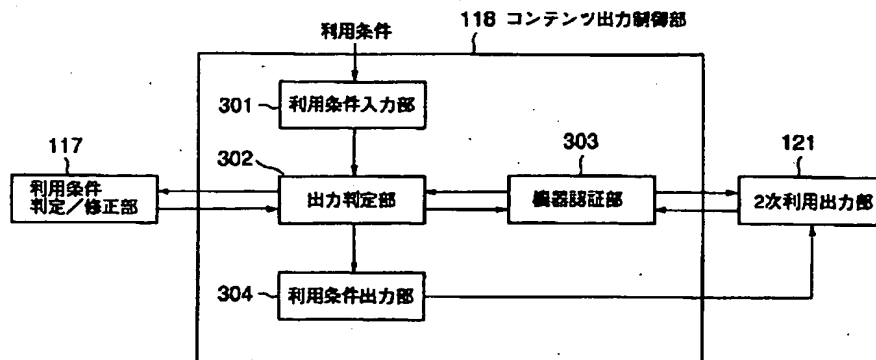
【図20】



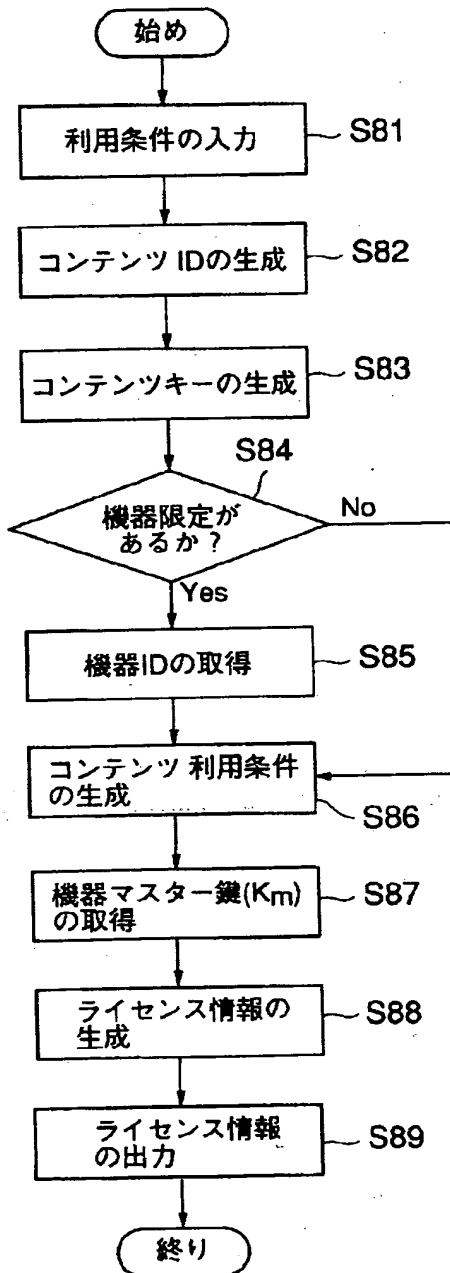
【図25】



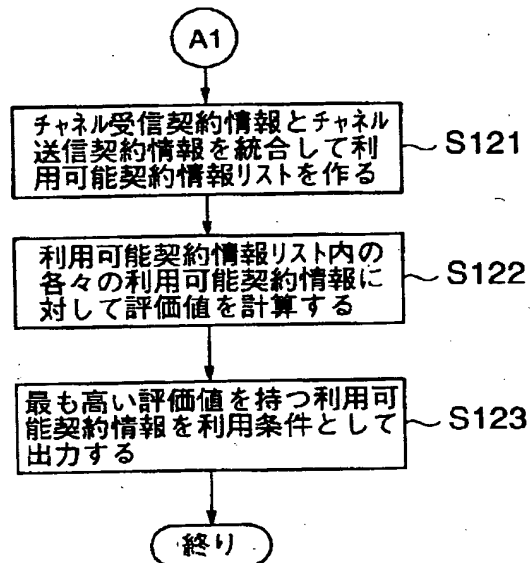
【図35】



【図 21】



【図 26】



【図 30】

有効期限情報	回数制限情報	機器限定情報	評価値
1999.05.20	-1	0	70
1999.06.10	-1	1	50
1999.06.10	15	1	50
1999.06.10	3	0	40
1999.05.20	3	1	20
1999.07.31	3	1	20
2000.01.07	3	1	120
-1	3	1	120
1999.05.20	10	0	70
1999.07.31	10	1	50
2000.01.07	10	1	150
2000.01.07	3	0	140

【図31】

利用可能契約情報選択画面

可能な利用形態は以下のものです。コンテンツの利用形態を選択して下さい。

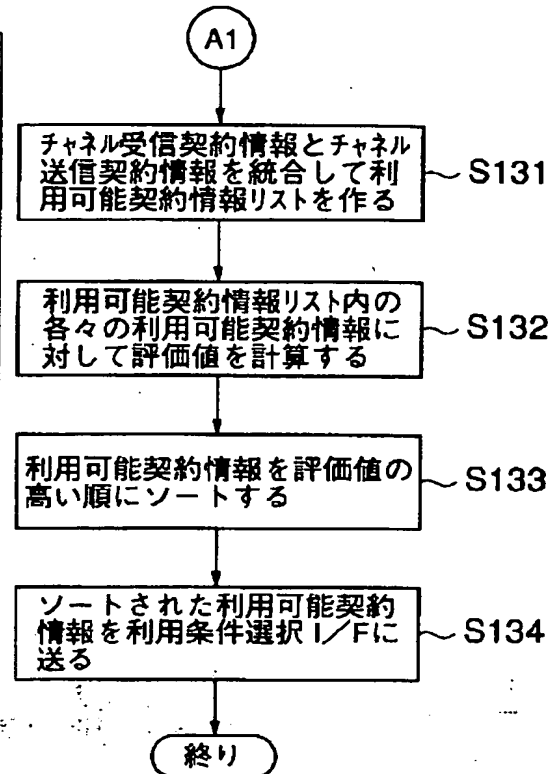
コンテンツ名

利用可能形態

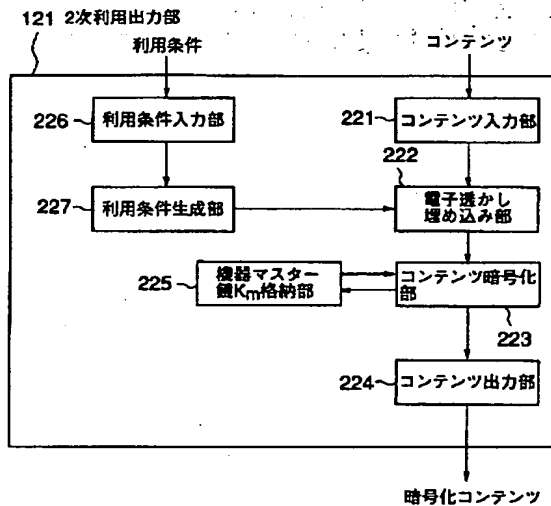
	有効期限	回数制限	機器固定
①	2000.01.07	10	あり
②	2000.01.07	3	なし
③	無期限	3	あり
④	2000.01.07	3	あり
⑤	1999.05.20	なし	なし

次の5件

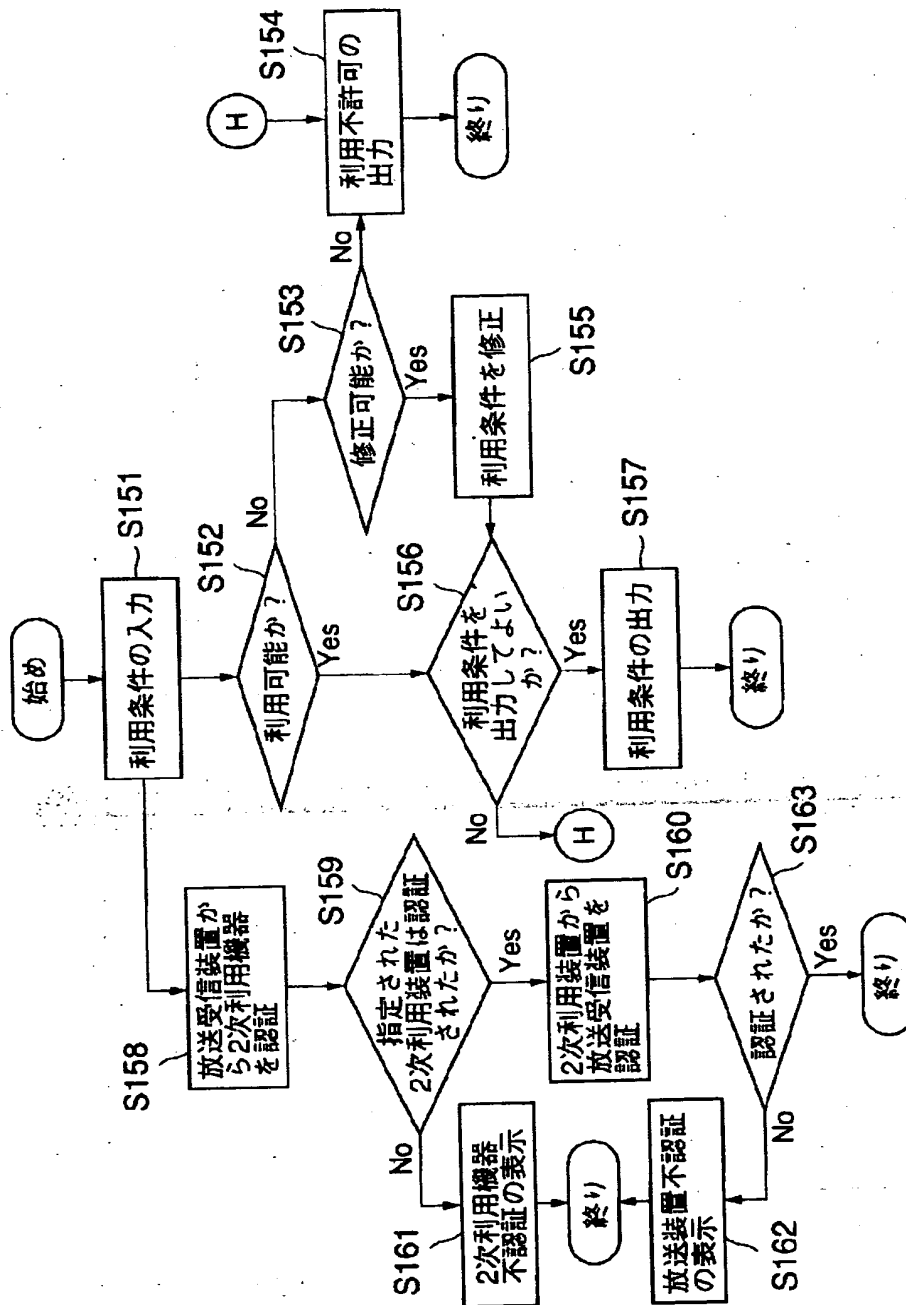
【図32】



【図33】

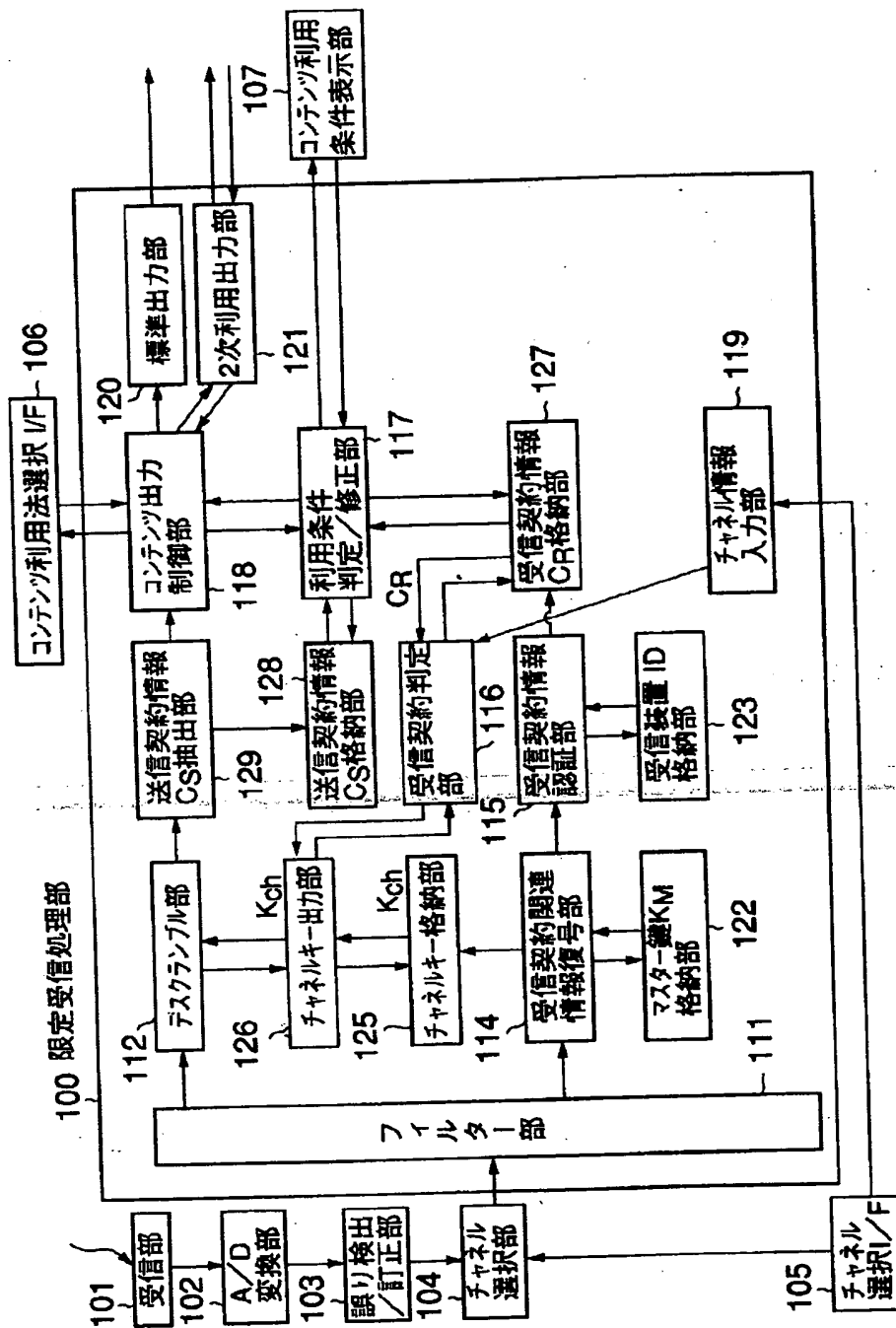


【図36】



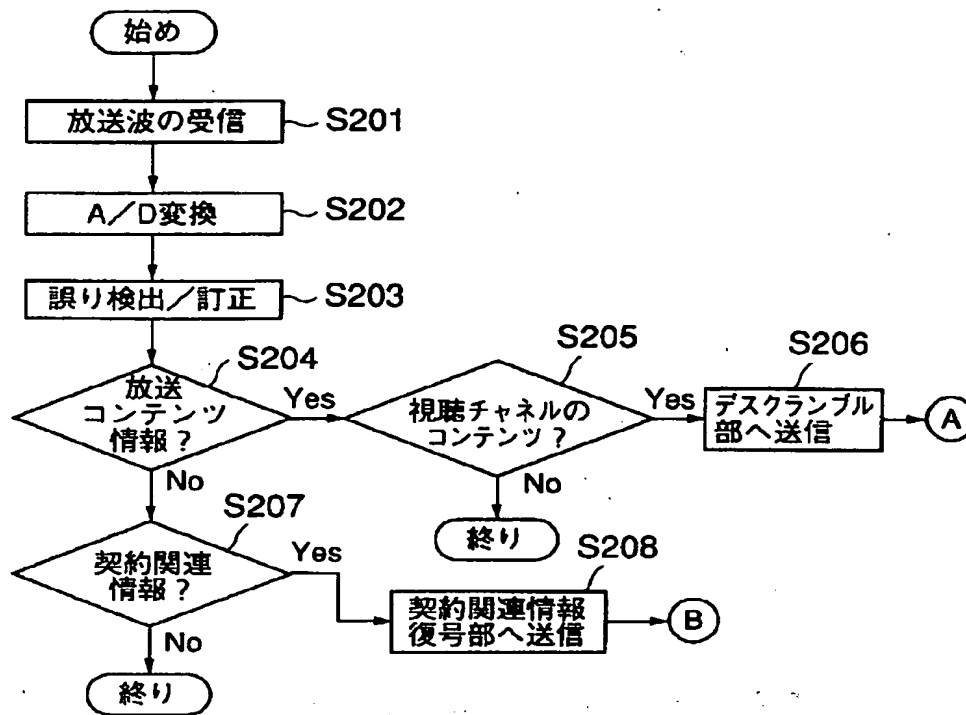


【図43】

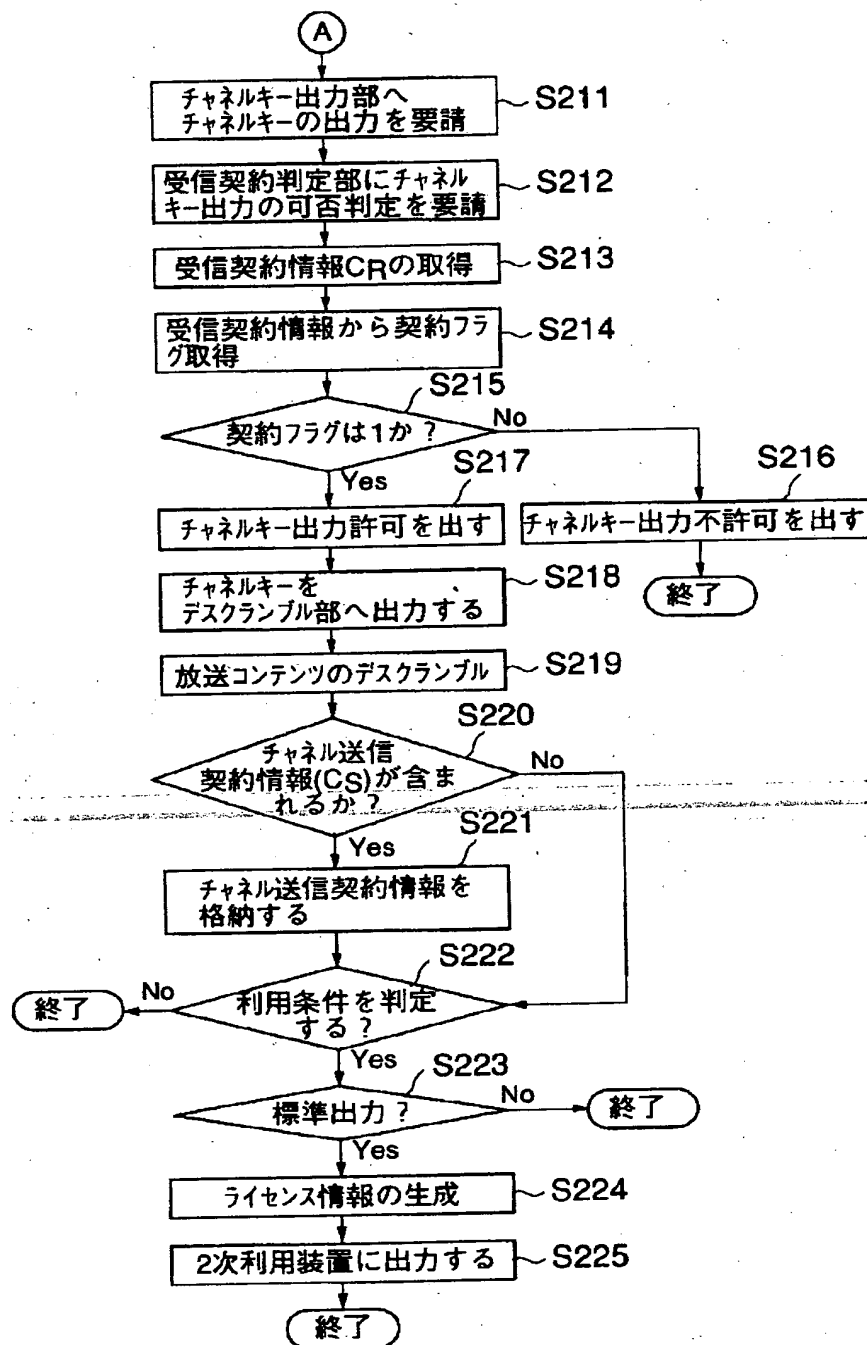




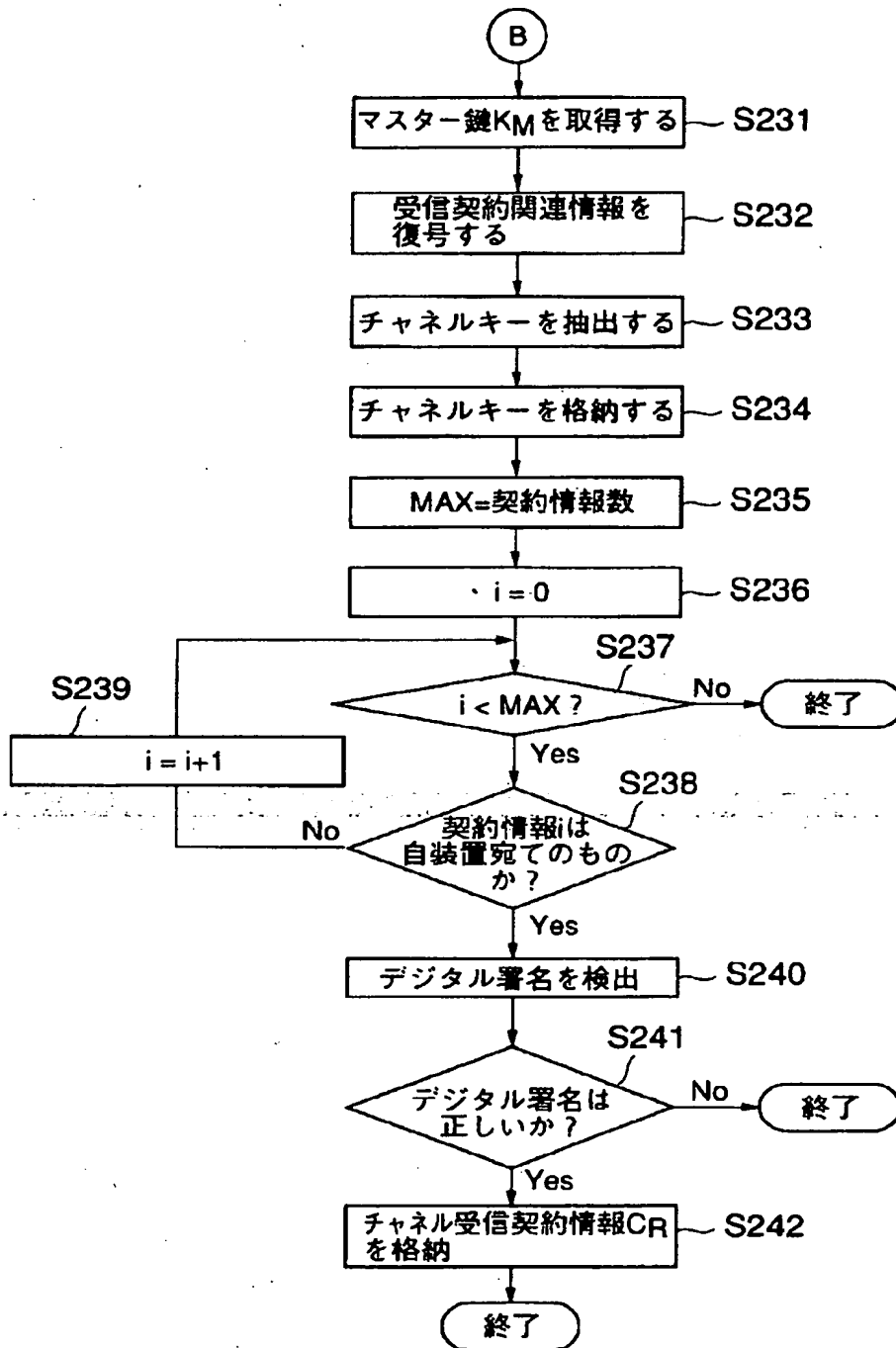
【図44】



【図45】



【図46】



フロントページの続き

(51) Int. Cl. 7

識別記号

F I

ターコード (参考)

H 0 4 N 7/16

H 0 4 L 9/00

6 0 1 E

6 8 5

Fターム (参考) 5C025 CB08 DA01 DA05  
5C064 BA01 BB05 BB07 BC06 BC20  
BD09 BD14  
5J104 AA01 BA03 DA03 EA01 EA06  
NA02 PA05  
5K061 AA00 AA12 BB17 BB19 DD00  
FF00 FF01 JJ03 JJ07